Sur quelques questions d'équidistribution en géométrie arithmétique

Rodolphe Richard

N° d'ordre : ANNÉE 2009

THÈSE / UNIVERSITÉ DE RENNES 1
sous le sceau de l'Université Européenne de Bretagne

pour le grade de

DOCTEUR DE L'UNIVERSITÉ DE RENNES 1

Mention : Mathématiques et Applications

Ecole doctorale Matisse

présentée par

Rodolphe Richard

préparée à l'unité de recherche UMR 6625 IRMAR
Institut de recherche mathématique de Rennes
UFR de Mathématiques

Sur quelques questions d'équidistribution en géométrie arithmétique

Thèse soutenue à Rennes
le jeudi 19 novembre 2009

devant le jury composé de :

Emmanuel Breuillard
Professeur, Université Paris-Sud 11 / rapporteur

Rutger Noot
Professeur, IRMA, Université Louis Pasteur, Strasbourg / rapporteur

Yves Guivarc'h
Professeur émérite, IRMAR, Université de Rennes 1 / examinateur

Bertrand Rémy
Professeur, Institut Camille Jordan, Lyon / examinateur

Emmanuel Ullmo
Professeur, Institut de Mathématiques d'Orsay, Paris sud 11 / examinateur

Antoine Chambert-Loir
Professeur, IRMAR, Université de Rennes 1 / directeur de thèse

Université de Rennes 1

N° d'ordre: 000

N° attribué par la bibliothèque

THÈSE

pour obtenir le grade de

Docteur de Université de Rennes 1

mention « **mathématique et applications** »

préparée à l'**Institut de recherche mathématique de Rennes**

dans le cadre de l'école doctorale **Matisse**

intitulée:

Sur quelques questions d'équidistribution en géométrie arithmétique

présentée et soutenue publiquement

par

Rodolphe Richard

le jeudi 19 novembre 2009

devant le Jury composé de:

M. ,	Président du jury
M. Emmanuel Breuillard,	Rapporteur
M. Rutger Noot,	Rapporteur
M. Yves Guivarc'h,	Examinateur
M. Bertrand Rémy,	Examinateur
M. Emmanuel Ullmo,	Examinateur
M. Antoine Chambert-Loir,	Directeur de thèse

Rodolphe RICHARD

SUR QUELQUES QUESTIONS D'ÉQUIDISTRIBUTION EN GÉOMÉTRIE ARITHMÉTIQUE

Rodolphe RICHARD
E-mail : rodolphe.richard@normalesup.org
Institut de recherche mathématique de Rennes, Université de Rennes 1,
35 000 Rennes.

TABLE DES MATIÈRES

Avant-Propos vii

Introduction ix
Équidistribution et hauteur de Weil ix
Équidistribution en géométrie d'Arakelov xii
Équidistribution et Courbes modulaires xiii
Équidistribution des points de Hecke xiv
Esquisse d'un mémoire xv

Résumé xvii

Bibliographie xxi

Partie I. Équidistribution galoisienne

Répartition galoisienne d'une classe d'isogénie de courbes elliptiques 3
1. Introduction 2
2. Courbes $Y(N)$, Action galoisienne et Énoncé 7
3. Action galoisienne sur une classe d'isogénie 9
4. Autour des réseaux arithmétiques maximaux 16
5. Équidistribution des points de Hecke 22
6. Démonstration 25
Bibliographie 27

Répartition galoisienne d'une classe d'isogénie de courbes elliptiques 31
Références 36

Équidistribution et Variétés de Shimura 37
Introduction 39

Mesures et Actions de groupe 40
Partie I. Variétés de Shimura 43
1. Quotients arithmétiques 43
2. Données de Shimura connexes 47
3. Variétés de Shimura complexes 51
4. Modèles canoniques, Action de Galois et Orbites de Hecke 54
Partie II. Propriétés d'équidistribution 56
5. Une Propriété de finitude sur les groupes arithmétiques 56
6. Équidistribution des points de Hecke 57
7. Cas adélique 59
Partie III. Répartition hyperbolique d'orbites de Hecke et d'orbites de Galois 60
8. Mesures hyperboliques 60
9. Équidistribution des points de Hecke 60
10. Équidistribution galoisienne 60
11. Espaces de modules de variétés abéliennes 61
Références 62

Partie II. Non divergence S-arithmétique

Geometric result on representations of reductive Lie groups 67
1. Main application 67
2. Preliminaries 69
3. Effective statements 74
4. Proof of Theorem 1 78
5. Postliminary enhancements: case of reductive G 80
Appendix A. Further remarks 80
References 84

Résultat géométrique sur les représentations de groupe réductifs sur un corps ultramétrique 87
1. Hypothèses et Énoncé 88
2. Notations 91
3. Propositions 93
4. Démonstration 97
Annexe 98
Appendice A. Variétés algébriques affines 99
Appendice B. Groupes algébriques affines, linéaires, réductifs 101
Appendice C. Corps locaux ultramétriques 103
Appendice D. Espace analytique 105
Appendice E. Immeuble euclidiens de Bruhat-Tits 110

Appendice F. Convexité 112
Références 116

On narrowness for translated algebraic probabilities in S-arithmetic homogeneous spaces 119
1. Non-divergence relative to semisimple S-Arithmetic lattices 120
2. Combination of [**RS09**] and [**Ric09**] 123
3. Preliminary Lemmas 124
4. Spaces of lattices, Mahler's criterion 126
5. A "good" parametrisation 127
6. Proof 129
References 130

AVANT-PROPOS

« Il est toujours aisé d'être logique.
Il est presque impossible d'être logique jusqu'au bout. »

A. Camus, *Le Mythe de Sisyphe*.

„ Nu credeam să-nvăț un mûri vrodată . . . ”

M. Eminescu, *Odă (în metru antic)*.

Ce mémoire est structuré de différents exposés, qui peuvent être lus indépendamment du point de vue didactique, et de la présente introduction, qui s'attache à en révéler l'unité sémantique. Aussi toute référence éventuelle d'un exposé aux autres exposés ne se fera qu'au même titre qu'une référence bibliographique. En revanche certains rappels généraux présents dans un exposé pourront être consultés à profit, mais pas nécessairement, pour accompagner la lecture d'un autre des exposés. Cela vaut particulièrement pour les lecteurs qui voudraient se familiariser avec les sujets traités.

Une première partie, composée des trois premiers exposés, traite de propriétés d'équidistribution galoisienne, en se basant sur la propriété d'équidistribution des points de Hecke. On y précise notamment un théorème de R. Pink sur une conjecture formulée dans [**Pin05**].

Une seconde partie, composée des trois derniers exposés, développe quelques résultats de non divergence, en généralisant une méthode et des résultats de A. Eskin, S. Mozès et N. Shah dans [**EMS97**].

INTRODUCTION

Ce mémoire présente divers résultats motivés par des question d'*équidistribution* en *géométrie arithmétique*.

Équidistribution et hauteur de Weil

De manière générale, nous entendons par « équidistribution » l'étude, *via* la théorie de la mesure, d'ensembles finis dans les espaces topologiques. La terminologie n'est pas consacrée, les termes de « répartition » ou d'« équirépartition » étant parfois interchangeablement utilisés, ce dernier terme soulignant de plus une idée d'homogénéité.

Un archétype de résultat d'équidistribution est donné, dans l'intervalle unité $[0;1]$ de la droite réelle, par la considération des parties fractionnaires d'un ensemble fini de nombres réels en progression arithmétique

$$E_n = \{x; x+a; \ldots; x+n\cdot a\}.$$

Lorsque le premier terme x et le pas a de la progression sont fixés, et pourvu que le pas a ne soit pas un nombre rationnel, les parties fractionnaires de cette progression s'équidistribuent dans l'intervalle unité lorsque n tend vers l'infini, au sens où pour toute fonction réelle continue et périodique de période 1 de la variable réelle f,

$$\lim_{n\to\infty} \frac{1}{n+1} \sum_{k=0}^{n} f(x+k\cdot a) = \int_0^1 f(t)\,dt.$$

Cette propriété se démontre directement.Elle peut être utilisée pour construire l'intégrale de Riemann.

Des énoncés plus généraux peuvent être démontrés en utilisant *le critère de Weyl*, savoir que l'équation

$$\lim_{n\to\infty} \frac{1}{|E_n|} \sum_{x\in E_n} f(x) = \int_0^1 f(t)\,dt$$

est satisfaite pour toute fonction f comme précédemment dès qu'elle est satisfaite pour tout polynôme trigonométrique, ou, plus précisément, pour les fonctions

$$t \mapsto \cos(kt) \text{ et } t \mapsto \sin(kt),$$

et ce pour tout entier naturel non nul k.

Il s'ensuit que, dans le plan complexe, les racines de l'équation $z^n = 1$, d'inconnue z, s'équidistribuent, lorsque l'entier n tend vers l'infini, le long du cercle unité pour la mesure d'angle : il suffit d'opérer le changement de variable $z = \exp(2\pi i t)$, le critère de Weyl revenant alors essentiellement à vérifier, en notations de Landau, l'identité

$$\sum_{z^n=1} z^k = o_n(n), \tag{1}$$

pour tout entier naturel non nul k. C'est bien le cas car, sauf si n divise k, la somme de gauche est nulle. Il s'agit en effet d'un diviseur de zéro : sa multiplication avec $\exp(2\pi i \cdot k/n) - 1$ produit une somme télescopique, de valeur totale nulle.

On peut affiner ce résultat en ne considérant que les racines *primitives* de l'unité de même ordre n. Il s'agit donc d'étudier les racines du polynôme cyclotomique Φ_n d'indice n plutôt que le polynôme $z^n - 1$. Les sommes

$$\sum_{\Phi_n(z)=0} z^k$$

sont alors les sommes symétriques de Newton sur les racines de Φ_n. De part les identités de Newton, la propriété d'équidistribution des racines primitives le long du cercle unité revient alors à une borne sur les les coefficients des polynômes cyclotomiques : pour tout entier naturel k non nul, la suite des coefficients de degré k du polynôme cyclotomique d'indice n est de classe $o_n(n)$. Par exemple, les coefficients non nuls de tous les polynômes cyclotomiques d'indice inférieur à 100 sont égaux à -1 ou $+1$.

La mesure d'angle se construit comme cas particulier de la notion plus générale de *mesure de Radon* sur le plan complexe : l'application

$$f \mapsto \int_0^1 f\big(\exp(2\pi i t)\big)\,dt$$

est bien définie sur l'espace des fonctions continues à support compact sur le plan complexe, et est une forme linéaire continue pour la topologie de la convergence

uniforme. Notons-la μ. Pour tout point z du plan complexe, l'application

$$f \mapsto f(z)$$

définit également une mesure de Radon : la masse de Dirac au point z, souvent notée δ_z. Pour toute partie finie F du plan complexe, la moyenne arithmétique

$$\frac{\sum_{e\in E}\delta_e}{|E|}$$

définit encore une mesure de Radon. Notons δ_E cette dernière. Nous dirons qu'une suite $(E)_{n\in\mathbf{N}}$ d'ensembles finis de nombre complexes *s'équidistribue vers la mesure de Radon* μ lorsque la suite $(\delta_{E_n})_{n\in\mathbf{N}}$ converge simplement vers μ. Autrement dit pour toute fonction continue à support compact f de la variable complexe,

$$\lim_{n\in\mathbf{N}} \frac{\sum_{e\in E_n} f(e)}{|E_n|} = \int_0^1 f(\exp(2\pi i t))\,dt.$$

Considérons une suite $(P_n)_{n\in\mathbf{N}}$ de polynômes irréductibles unitaires à coefficients entiers dont la suite de lieux des zéros

$$(E_n)_{n\in\mathbf{N}} = \big(\{z\in\mathbf{C}\big|P_n(z)=0\}\big)_{n\in\mathbf{N}}$$

s'équidistribue vers la mesure d'angle μ. Introduisons la *mesure de Mahler* d'un polynôme P_n unitaire à coefficient entiers et racines simples : il s'agit du produit

$$M(P_n) = \prod_{P_n(z)=0} \max\{1;|z|\}.$$

Notons que $M(P_n)$ a pour logarithme $\sum_{P_n(z)=0}\log^+|z|$, où la fonction $\log^+|-| : z\mapsto \max\{0;\log(z)\}$ désigne la partie positive, prolongée par 0 en l'origine, du logarithme de la valeur absolue $|-| : \mathbf{C}\to\mathbf{R}$. Comme la suite $(E_n)_{n\in\mathbf{N}}$ s'équidistribue vers la mesure d'angle μ, l'identité

$$\lim_{n\in\mathbf{N}} \frac{\sum_{P(z)=0}\log^+|z|}{|E_n|} = \int_0^1 \log^+\big|\exp(2\pi i t)\big|\,dt$$

s'applique encore, car la fonction $\log^+|-|$ est positive.

Rappelons que le cardinal $|E_n|$ vaut le *degré* du polynôme P_n. On appelle la quantité

$$h(P) = \frac{M(P)}{\deg(P)}$$

hauteur (logarithmique de Weil) des racines de P. Elle sert de mesure de la « complexité arithmétique » des entiers algébriques : en vertu d'un théorème de Northcott, il n'existe qu'un nombre fini d'entiers algébriques du plan complexe de degré et de hauteur bornés. Plus précisément, les coefficients du polynôme minimal unitaire d'un entier algébrique sont des entiers relatif dont la valeur absolue peut être effectivement bornée en terme de la hauteur. Ainsi la propriété d'équidistribution

des racines de P vers la mesure d'angle μ implique que la hauteur de ces racines tend vers 0 : on parle de (suite de) points de petite hauteur, ou encore de *petits points*. Par exemple, la hauteur des racines de l'unité est nulle.

Un théorème de Y. Bilu, dans [**Bil97**], contient l'implication réciproque : si la hauteur d'une suite suite $(z_n)_{n\in\mathbf{N}}$ d'entiers algébriques (distincts), de polynômes minimaux respectifs P_n, tend vers zéro, alors la suite $(\{z \in \mathbf{C} | P_n(z) = 0\})_{n\in\mathbf{N}}$ des ensembles de racines de leur polynôme minimal s'équidistribue vers la mesure d'angle μ sur le cercle unité. C'est bien le cas pour une suite $(z_n)_{n\in\mathbf{N}}$ formée de racines de l'unité distinctes.

Équidistribution en géométrie d'Arakelov

Un énoncé emblématique en géométrie arithmétique est la *conjecture de Mordell*. Cette conjecture énonce une conséquence arithmétique, la finitude du nombre de solution en nombres rationnels d'une équation diophantienne, à partir d'une hypothèse géométrique, que la variété des solutions complexes de l'équation forme une surface de Riemann complète hyperbolique. En guise d'illustration, indiquons que, considérant la courbe d'équation

$$X^N + Y^N = 1,$$

cette conjecture implique directement, pour chaque entier N au moins égal à 3, la *finitude* du nombre de contre-exemples au théorème de Fermat (comptés à proportionnalité près). La condition sur N provient de l'hypothèse géométrique, alors que la conséquence est de nature arithmétique.

La célèbre preuve de G. Faltings ([**Fal83**]) passe par la *géométrie d'Arakelov*. Une caractéristique de la géométrie d'Arakelov est la considération de métriques hermitiennes sur les fibrés en droites, et de définir ainsi une notion très souple et générale de *hauteur*. Faltings, dans le contexte des espaces de modules de variétés abéliennes, définit ainsi la *hauteur de Faltings*, un outil central dans sa démonstration de la conjecture de Mordell.

La *conjecture de Bogomolov* ([**Bog80**]) pose, sous la même hypothèse géométrique, une autre question arithmétique : l'étude des solutions *algébriques* de ces équations diophantiennes, nécessairement en nombre infini, en terme de leur hauteur. Plus précisément elle affirme que, quitte à éviter un nombre *fini* de solutions, la hauteur de Néron-Tate de ces solutions ne peut s'approcher de zéro.

Le théorème de Bilu rentre dans le cadre de développements récents en géométrie d'Arakelov, marqués par la preuve de la conjecture de Bogomolov par E. Ullmo ([**Ull98**]). La preuve d'Ullmo déduit la conjecture de Bogomolov d'un énoncé général d'équidistribution de « petits points » ([**SUZ97**]).

Cet énoncé d'équidistribution combine deux arguments de géométrie d'Arakelov.

Le premier est un analogue en géométrie d'Arakelov du théorème de Hilbert-Samuel de la géométrie algébrique. Rapellons, qu'en géométrie algébrique, le théorème de Hilbert-Samuel concerne la dimension asymptotique de l'espace des sections globales des puissances successives d'un fibré en droites ample. En géométrie d'Arakelov, il s'agit plutôt d'estimer le nombre de sections globales bornées (pour une métrique positive fixée sur le fibré).

Le second argument est un principe variationnel ([**SUZ97**]) : il consiste à étudier, au premier ordre, l'évolution des énoncés précédent lorsque l'on varie la métrique considérée.

Ces méthodes ne s'appliquent qu'aux suites (« génériques ») de points algébriques dont la hauteur tend vers un minimum prescrit.

Équidistribution et Courbes modulaires

Un résultat que nous établissons dans le premier exposé de ce mémoire construit des familles de points algébriques dans les courbes modulaires qui présentent des propriétés d'équidistribution analogues aux précédentes, mais qui ne rentrent pas dans le cadre des méthodes précédentes.

Par exemple, nous construisons des suites d'entiers algébriques complexes $(j_n)_{n\in\mathbf{N}}$ telles que, notant E_n l'ensemble des conjugués algébriques de j_n, la suite $(E_n)_{n\in\mathbf{N}}$ s'équidistribue vers une mesure à densité $d(z)\,|dz|$ sur le plan complexe. Nous renvoyons à l'introduction de ce premier exposé pour la définition des suites considérées, de la mesure à densité et un énoncé précis de notre résultat.

Mentionnons que pour une suite générale de nombres algébriques, la suite $(E_n)_{n\in\mathbf{N}}$ correspondante n'a en général pas propriété particulière. Par exemple une suite de nombres rationnels ne converge que s'il s'agit d'une suite de Cauchy, et dans ce cas la mesure limite est une masse de Dirac.

En particulier, notre résultat implique que le degré des nombres j_n tend vers l'infini. Ce corollaire est en fait un ingrédient de notre démonstration. Plus exactement, nous utilisons un théorème plus précis, dû à J.-P. Serre, qui décrit le degré algébrique des nombres j_n considérés ([**Ser68**],[**Ser72**]). Notre méthode s'applique également aux nombres complexes transcendants, auquel cas on se base sur des travaux de Shimura sur le groupe fondamental des courbes modulaires elliptiques.

Un calcul direct montre que cette densité $d(z)$ a comme équivalent $\frac{1}{|z|^2(\log^+|z|)^2}$. Par conséquent la sommabilité de la fonction $\log^+|-|$ se ramène, en coordonnée radiale r, à celle l'intégrale de Bertrand $\int \frac{1}{r}\frac{1}{\log(r)}dr$ au voisinage de l'infini : l'intégrale $\int_{\mathbf{C}} \log^+|z|\cdot d(z)\,|dz|$ est infinie. Il s'ensuit que la hauteur des nombres j_n tend vers l'infini.

Remarquons que la fonction $\log^+|-|$ de classe $L^{1-\epsilon}\big(d(z)\,|dz|\big)$ pour tout ϵ de l'intervalle unité ouvert $]0;1[$. En comparant la hauteur de j_n à la moyenne empirique de $\deg(P_n)$ tirages indépendants de la variable aléatoire de même loi que $\log^+|-|\cdot d(z)\,|dz|$, notre résultat d'équidistribution suggère, par analogie avec [**Rau00**], un équivalent pour la suite de hauteurs $\big(h\big(j_n\big)\big)_{n\in\mathbf{N}}$.

Pour les points considérés, ces hauteurs ont été calculées précisément (et même exactement quitte à changer la notion de hauteur) par E. Ullmo et L. Szpiro, en utilisant, outre le résultat de Serre mentionné précédemment, et des méthodes de géométrie d'Arakelov ([**SU99**]). Toutefois notre résultat d'équidistribution ne découle pas de méthodes de géométrie d'Arakelov concernant les petits points, car la hauteur de la suite $\big(j_n\big)_{n\in\mathbf{N}}$ s'élève indéfiniment.

Notre énoncé complète un théorème de W. Duke, qui, dans [**Duk88**], développe des méthodes de théorie analytique des nombres introduites par H. Iwaniec concernant les coefficients de Fourrier des formes modulaires. Cependant nos méthodes ne s'appliquent pas *a pripori* dans le cas considéré par Duke.

En fait les méthodes que nous introduisons ne rélèvent ni de la géométrie d'Arakelov, ni de la théorie analytique des nombres. Le second ingrédient principal de notre démonstration, outre le théorème de Serre, repose sur une reformulation de la propriété d'*équidistribution des points de Hecke*, que l'on peut démontrer en se basant sur des méthodes d'analyse harmonique ([**COU01**]) ou bien de théorie ergodique ([**EO06**]). Pour introduire cet ingrédient, revenons à l'exemple de l'équidistribution des racines de l'unité.

Équidistribution des points de Hecke

L'application $x \mapsto \exp(2\pi i x)$ envoie le groupe additif $\mathbf{R}$ vers le groupe multiplicatif $\mathbf{C}^\times$. C'est un morphisme de groupes, et son noyau est le sous-groupe discret formé par l'ensemble $\mathbf{Z}$ des entiers relatifs. Les racines de l'unité sont exactement les images des points rationnels de la droite réelle. Les points rationnels non nuls sont également les éléments q du groupe additif réel qui engendrent un sous-groupe $q\mathbf{Z}$ d'intersection non nulle avec $\mathbf{Z}$. En outre les sous-groupes obtenus ainsi sont les sous-groupes *commensurables* avec $\mathbf{Z}$ au sens où $q\mathbf{Z}$ et $\mathbf{Z}$ ont une intersection qui est d'indice fini dans $\mathbf{Z}$ et dans $q\mathbf{Z}$. L'équidistribution des racines de l'unité se reformule alors comme suit : les sous-groupes finis d'ordre de plus en plus grand du groupe quotient $\mathbf{R}/\mathbf{Z}$ s'équidistribuent vers la mesure invariante par translation (la mesure de Lebesgue).

La propriété d'*équidistribution des points de Hecke* généralise cette propriété à des groupes plus généraux que le groupe additif réel. Notre démonstration, dans notre premier exposé, se restreint au cas du groupe $SL(2,\mathbf{R})$. Rappelons qu'il s'agit du groupe formé des transformations linéaires du plan vectoriel réel qui préservent

l'orientation et la forme d'aire. L'ensemble sous-jacent à ce groupe est une hypersurface quadratique dans l'espace vectoriel des endomorphismes du plan vectoriel : il est déterminé, dans les coordonnées $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ par l'équation $ad - bc = 1$ sur le déterminant jacobien.

Le sous-ensemble de $SL(2,\mathbf{R})$ formé des automorphismes du plan dont la matrice est à coefficients entiers définit un sous-ensemble discret, car les entiers sont isolés dans la droite réelle. C'est également un sous-groupe, en vertu de la loi de multiplication des matrices, et de la formule de Cramer

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Ce sous-groupe, $SL(2,\mathbf{Z})$, est également caractérisé comme le stabilisateur, dans $SL(2,\mathbf{R})$, du réseau vectoriel formé des points du plan à coordonnées entières. Les réseaux vectoriels R de $\mathbf{R}^2$ que l'on obtient comme image de $\mathbf{Z}^2$ sous l'action d'au moins un élément de $SL(2,\mathbf{R})$ sont les réseaux dont les parallélogrammes fondamentaux sont de volume 1. Il est équivalent de dire que le quotient $\mathbf{R}^2/R$ pour la métrique induite par la distance euclidienne standard sur $\mathbf{R}^2$ est une surface d'aire 1. On dit que le réseau R est unimodulaire. L'application $g \mapsto g(\mathbf{Z}^2)$ identifie alors le quotient $SL(2,\mathbf{R})/SL(2,\mathbf{Z})$ à l'ensemble des réseaux vectoriels unimodulaires du plan.

L'ensemble quotient $SL(2,\mathbf{R})/SL(2,\mathbf{Z})$ est muni de l'action induite à gauche du groupe $SL(2,\mathbf{R})$. Les orbites de Hecke désignent les orbites de $SL(2,\mathbf{Z})$ dans $SL(2,\mathbf{R})/SL(2,\mathbf{Z})$ qui sont *finies*. Les réseaux vectoriels qui sont situés sur les orbites de Hecke sont précisément les réseaux qui sont proportionnels à un réseau commensurable à $\mathbf{Z}^2$. La propriété d'équidistribution des points de Hecke affirme qu'une suite d'orbites de Hecke de cardinal de plus en plus grand s'équidistribue vers une mesure de probabilité invariante, et donc nécessairement unique, sous l'action de $SL(2,\mathbf{R})$.

Comme nous le faisons remarquer, il se trouve que cette condition sur les cardinaux des orbites est automatiquement vérifiée : pour une suite d'orbites de Hecke deux-à-deux distinctes, le cardinal tend nécessairement vers l'infini.

Esquisse d'un mémoire

Terminons cette introduction en indiquant comment les travaux de ce mémoire s'inscrivent dans la perspective que nous venons dresser.

Tout d'abord nous montrons comment le résultat déjà évoqué se généralise, du contexte des courbes modulaires à celui, plus large, des « variétés de Shimura ».

Ce contexte englobe en particulier de nombreux espaces de modules de variétés abéliennes.

L'un de nos ingrédients vaut en toute généralité dans ce contexte, il s'agit de l'équidistribution des points de Hecke. En revanche, la généralisation du théorème de Serre à ce contexte se ramène à une variante de la conjecture de Mumford-Tate. C'est une question centrale qui a déjà fait l'objet de nombreux travaux. Concernant les espaces de variétés abéliennes, la conjecture de Tate, démontrée par Faltings, fournit déjà de précieux renseignements sur les orbites étudiées.

C'est pourquoi dans la seconde partie de ce mémoire, nous essayons d'affiner la propriété d'équidistribution des points de Hecke. À cette fin, nous pouvons compter sur la grande souplesse des théorèmes de Ratner pour identifier les mesures limites qui se présenteraient. Mais, suivant les travaux d'Eskin, Mozès et Shah, il nous faut d'abord démontrer l'existence de mesures limites.

La seconde partie de ce mémoire généralise les résultats de ces auteurs au contexte S-arithmétique. Cette partie étant partiellement rédigée en anglais, nous l'avons décrite avec plus de détails dans le résumé qui suit. Nous nous y référons pour une description plus technique du contenu de cette partie.

Mentionnons pour terminer l'une des motivations de nos travaux. Il s'agit de l'analogie, en termes de centralisateurs des groupes considérés, entre la conclusion de la conjecture de Tate et l'hypothèse des résultats d'Eskin, Mozès et Shah.

RÉSUMÉ

La première partie de ce mémoire est formée des trois premiers exposés.

Le premier exposé relie les constructions précédentes à l'action du groupe de Galois sur des invariants de courbes elliptiques complexes variant dans une même classe d'isogénie. Il s'agit du texte d'un article de recherche soumis et en cours de relecture. Nous renvoyons à son introduction pour la définition de ces objets et l'énoncé précis du résultat démontré. Le second exposé est le texte d'une note en cours de publication aux comptes-rendus de l'Académie des sciences, et résume le contenu du premier exposé.

Le troisième exposé quant à lui présente dans le détail et en grande généralité les applications des méthodes que nous avons utilisées dans le premier exposé. Nous étendons notamment un théorème de R. Pink ([**Pin05**]) aux variétés de Shimura en général, et précisons la conjecture correspondante, au sens où l'on démontre une propriété d'équidistribution, plutôt que de densité de Zariski. On répond ainsi à certaines remarques de R. Pink. Nous revenons en détail sur les définitions et outils utilisés et, le cas échéant, fixons les conventions utilisées parmi les différents usages qui ressortent de la littérature existante.

La seconde partie de ce mémoire présente une série de trois articles sur des questions liées à des propriétés de non divergence dans les espaces de réseaux, au sens de [**EMS97**]. La motivation principale est, en combinaison avec le théorème de Ratner, d'affiner la propriété d'équidistribution des points de Hecke. Toutefois les démonstrations que nous développons nécessitent des outils variés, et démontrent des résultats intermédiaires d'intérêt propre. Les résultats démontrés ont des applications, en cours de rédaction, aux questions traitées dans la première partie.

Le premier exposé de cette partie, le quatrième de ce mémoire, présente un résultat qui est le fruit d'une collaboration avec le Pr Nimish Shah, datant d'une visite

au *Tata Insitute of fundamental Research* de Mumbaï, en 2005 en Inde. À ce titre, il est rédigé en anglais, d'autant plus qu'il est destiné à être publié, tel quel, comme article de recherche ; nous en donnons un bref résumé en français. Que le TIFR et Nimish reçoivent ici mes plus sincères remerciements, ne serait-ce que parce que les questions étudiées dans cette thèse tirent leur source de réflexions entamées à cette occasion.

Le résultat principal de cet exposé répond à une question que N. Shah avait soulevé, et les étapes principales de la démonstration sont le fruit de notre collaboration. La rédaction que nous présentons présente ces arguments sous un jour différent, et explicite le caractère effectif de la preuve. Un des théorèmes que nous démontrons est une généralisation directe d'une proposition de [**EMS97**]. Il répond au problème suivant.

On considère un groupe de d'endomorphismes H d'un espace vectoriel réel V de dimension finie et une partie Ω de H. Pour tout vecteur v de V, $\Omega \cdot v$ est donc une partie de l'orbite de H en v. Étant donné un automorphisme g dans $GL(V)$, on considère l'image $g\Omega v$ de cette partie sous l'action de g. La question est de savoir, en termes de g, si g peut envoyer uniformément l'ensemble $\Omega \cdot v$ vers l'origine de V. Plus précisément, étant donné une norme $\|-\|$ sur V, on décrit un ensemble d'éléments g de $GL(V)$ tel que pour tout vecteur v, on a une minoration

$$\sup_{\omega \in \Omega} \|g\omega v\| \geq \|v\| / c$$

pour une constante positive et inversible c qui est uniforme.

Remarquons tout d'abord que lorsque z appartient au commutant de H, l'identité $z\Omega v = \Omega z v$ implique, disons si Ω est compact, que la partie $z\Omega v = \Omega z v$ converge uniformément vers l'origine de V si et seulement si $\|zv\|$ tend vers 0. C'est par exemple le cas si z décrit des homothéties dont le rapport tend vers 0.

Le contexte dans lequel notre énoncé se situe est celui d'un sous-groupe H d'un groupe G, le groupe G agissant linéairement sur V. Nous considérons également des hypothèses supplémentaires sur les groupes G et H, comme le fait ce soient des groupes de Lie réductifs. Nous décrivons alors un sous-ensemble Y de G complémentaire au centralisateur $Z_G(H)$ de H dans G, au sens où $G = YZ_G(H)$ et tel que l'inégalité

$$\sup_{\omega \in \Omega} \|y\omega v\| \geq \|v\| / c$$

soit vérifiée pour une constante positive et inversible c qui est uniforme lorsque y décrit Y. Bien sûr il faut également quelques hypothèses sur Ω. Celles que nous donnons semblent optimales. Elles sont en particulier vérifiées si Ω est d'intérieur non vide, voire de mesure non nulle, ou encore Zariski dense.

La proposition originale de [**EMS97**] ne considérait que le cas où H est un tore algébrique réel. En utilisant notre résultat à la place de cette proposition, nous simplifions grandement la démonstration du théorème principal de [**EMS97**]. En combinaison avec un théorème de D. Kleinbock et G. Tomanov ([**KT07**]), nous démontrons même immédiatement, dans le sixième exposé, une généralisation du résultat principal de [**EMS97**].

Le cinquième exposé adapte les méthodes du quatrième exposé au contexte des corps locaux ultramétriques. Le problème étudié précédemment s'énonce en effet sans changement sur tout corps local, pour peu que l'on remplace les groupes de Lie réels par des groupes de points rationnels de groupes algébriques. Nous démontrons le théorème correspondant.

Toutefois, si la stratégie de démonstration est, dans l'essentiel, la même, notre démonstration est moins effective. Certain des outils qui étaient utilisés sont propres à l'analyse archimédien et n'ont pas d'analogue direct dans le contexte ultramétrique. Il s'agit de la propriété de convexité de la fonction exponentielle, qui n'est plus partout convergente dans le cas p-adique, et de la décomposition de Mostow qui généralise la décomposition polaire de Cartan. La preuve dans le contexte ultramétrique est assez récente, et n'a pu être menée à bout qu'en invoquant deux outils plutôt sophistiqués : les immeubles de Bruhat-Tits et la géométrie analytique au sens de Berkovich.

Dans le cas des groupes classiques, l'article [**BT84**] donne déjà des interprétations des immeubles en termes d'espaces de normes sur des objets classiques. Dans le cadre des groupes *réductifs* déployés (dits « de Chevalley » dans [**Ber90**], « de Demazure » chez [**RTW09**]), V. Berkovich relie explicitement l'immeuble de Bruhat-Tits étendu avec spectres de Banach ultramétriques, formés d'espaces de semi-normes multiplicatives. Ce n'est que dans le travail récent [**RTW09**], en cours de finalisation, de B. Rémy, A. Thuillier et A. Werner que l'on retrouve en très grande généralité, généralité suffisante pour le cas des corps locaux ultramétriques que nous considérons, la constructions de plongement équivariants des immeubles dans les espaces analytiques des schémas en groupes correspondants.

Toutefois la construction de [**RTW09**], dans le cas qui nous intéresse, n'est *a priori* pas explicite. Nous somme amenés à conduire quelques lemmes afin de vérifier une propriété de convexité des fonctions régulières sur l'espace analytique relativement à la structure affine de l'immeuble que l'on plonge. Il semble que cette propriété s'inscrive dans les développements récents en géométrie tropicale p-adique. Nous la démontrons directement. Cette propriété est immédiate dans la construction donnée par Berkovich. Nous nous inspirons du travail de Berkovich, dans [**Ber90**] pour vérifier, nous basant sur les propriétés générales des constructions de [**RTW09**], que cette propriété de convexité est également vérifiée en toute généralité. Nous ramenons en fait cette propriété de convexité à un analogue de

la convexité du polygone de Newton. Pour cela la géométrie au sens de Berkovich aurait pu être remplacée par la géométrie rigide, par exemple au sens de Tate. Ce sont ces propriétés de convexités qui vont remplacer l'usage de la fonction exponentielle du quatrième exposé.

Un autre outil que nous sommes amenés à adapter est la décomposition de Mostow. Pour obtenir un analogue, moins précis et sous des hypothèses plus restrictives, mais suffisant pour nos applications, nous utilisons les propriétés d'« hyperbolicité » des immeubles, plus précisément l'existence d'une métrique de Hadamard compatible à la structure affine et invariante sous l'action du groupe opérant. Plus précisément encore nous utilisons l'existence de points fixes de groupes d'isométries compacts sur des convexes fermés. Pour cette raison l'utilisation d'espace complets et localement compacts préconise le choix de la géométrie analytique au sens de Berkovich. D'autant plus que notre utilisation de la géométrie ultramétrique se fait par l'intermédiaire de normes multiplicatives. Mentionnons enfin que notre décomposition de l'immeuble couvre, masi pas seulement, le cas des décompositions subordonnées aux sous-groupes symétriques (groupes des points fixe d'une involution).

Le sixième exposé combine les résultats des deux précédents exposés avec la méthode de Dani-Margulis, dans la généralité développée dans [**KT07**], afin de généraliser les résultats de [**EMS97**] dans plusieurs directions. Nous indiquons en particulier comment certains résultats intermédiaires de [**EMS97**], qui utilisent la méthode de Dani-Margulis, entrent dans le cadre axiomatique de [**KT07**].

Nous sommes également appelés à démontrer quelques lemmes qui permettent de généraliser à des groupes linéaires généraux un énoncé de [**KT07**] qui ne concerne que les groupes unipotents.

BIBLIOGRAPHIE

[Ber90] V. G. BERKOVICH – *Spectral theory and analytic geometry over non-Archimedean fields*, Mathematical Surveys and Monographs, vol. 33, American Mathematical Society, Providence, RI, 1990.

[Bil97] Y. BILU – « Limit distribution of small points on algebraic tori », *Duke Math. J.* **89** (1997), no. 3, p. 465–476.

[Bog80] F. A. BOGOMOLOV – « Points of finite order on abelian varieties », *Izv. Akad. Nauk SSSR Ser. Mat.* **44** (1980), no. 4, p. 782–804, 973.

[BT84] F. BRUHAT & J. TITS – « Schémas en groupes et immeubles des groupes classiques sur un corps local », *Bull. Soc. Math. France* **112** (1984), no. 2, p. 259–301.

[COU01] L. CLOZEL, H. OH & E. ULLMO – « Hecke operators and equidistribution of Hecke points », *Invent. Math.* **144** (2001), no. 2, p. 327–351.

[Duk88] W. DUKE – « Hyperbolic distribution problems and half-integral weight Maass forms », *Invent. Math.* **92** (1988), no. 1, p. 73–90.

[EMS97] A. ESKIN, S. MOZES & N. SHAH – « Non-divergence of translates of certain algebraic measures », *Geom. Funct. Anal.* **7** (1997), no. 1, p. 48–80.

[EO06] A. ESKIN & H. OH – « Ergodic theoretic proof of equidistribution of Hecke points », *Ergodic Theory Dynam. Systems* **26** (2006), no. 1, p. 163–167.

[Fal83] G. FALTINGS – « Endlichkeitssätze für abelsche Varietäten über Zahlkörpern », *Invent. Math.* **73** (1983), no. 3, p. 349–366.

[KT07] D. KLEINBOCK & G. TOMANOV – « Flows on S-arithmetic homogeneous spaces and applications to metric Diophantine approximation », *Comment. Math. Helv.* **82** (2007), no. 3, p. 519–581.

[Pin05] R. PINK – « A combination of the conjectures of Mordell-Lang and André-Oort », in *Geometric methods in algebra and number theory*, Progr. Math., vol. 235, Birkhäuser Boston, Boston, MA, 2005, p. 251–282.

[Rau00] A. RAUGI – « Dépassement des sommes partielles de v.a.r. indépendantes équidistribuées sans moment d'ordre 1 », *Ann. Fac. Sci. Toulouse Math. (6)* **9** (2000), no. 4, p. 723–734.

[Ric09] R. RICHARD – « Résultat géométrique sur les représentations de groupes algébriques réductifs sur un corps ultramétrique », *Cette thèse* (2009).

[RS09] R. RICHARD & N. SHAH – « Résultat géométrique sur les représentations de groupes de Lie réductifs », *Cette thèse* (2009).

[RTW09] B. RÉMY, A. THUILLIER & A. WERNER – « Bruhat-Tits theory from Berkovich's point of view. I - Realizations and Compactifications of buildings », *Prépublication* (2009).

[Ser68] J.-P. SERRE – *Abelian l-adic representations and elliptic curves*, McGill University lecture notes written with the collaboration of Willem Kuyk and John Labute, W. A. Benjamin, Inc., New York-Amsterdam, 1968.

[Ser72] _____, « Propriétés galoisiennes des points d'ordre fini des courbes elliptiques », *Invent. Math.* **15** (1972), no. 4, p. 259–331.

[SU99] L. SZPIRO & E. ULLMO – « Variation de la hauteur de Faltings dans une classe de $\overline{\mathbf{Q}}$-isogénie de courbe elliptique », *Duke Math. J.* **97** (1999), no. 1, p. 81–97.

[SUZ97] L. SZPIRO, E. ULLMO & S. ZHANG – « Équirépartition des petits points », *Invent. Math.* **127** (1997), no. 2, p. 337–347.

[Ull98] E. ULLMO – « Positivité et discrétion des points algébriques des courbes », *Ann. of Math. (2)* **147** (1998), no. 1, p. 167–179.

PARTIE I

ÉQUIDISTRIBUTION GALOISIENNE

Répartition galoisienne d'une classe d'isogénie de courbes elliptiques

Rodolphe Richard

November 16, 2009

Résumé

Dans cet article, on montre que les orbites sous Galois des invariants associés à des courbes elliptiques complexes *sans multiplication complexe* variant dans *une même classe d'isogénie* s'équidisitribuent dans la courbe modulaire vers la probabilité hyperbolique. La démonstration repose sur des arguments de théorie ergodique, notamment le *théorème de Ratner* (cf. [9]), ainsi que sur le *théorème de l'image ouverte de Serre* ([19] et [20]) dans le cas où les invariants j considérés sont algébriques sur $\mathbf{Q}$, et des résultats de G. Shimura dans le cas transcendant ([22]).

Abstract

In this article, one shows that Galois orbits of invariants associated with *non CM* and *pairwise isogeneous* complex elliptic curves equidistribute in the classical modular curve towards the hyperbolic probability measure. The proof is based on arguments from ergodic theory, especially *Ratner's theorem on unipotent flows* (cf. [9]), as well as on *Serre's open image theorem* ([19] et [20]) in case of algebraic invariants, and on G. Shimura's work in the transcendant case ([22]).

Table des matières

1 Introduction **2**

2 Courbes $Y(N)$, Action galoisienne et Énoncé **7**

3 Action galoisienne sur une classe d'isogénie **9**

4 Autour des réseaux arithmétiques maximaux **16**

5 Équidistribution des points de Hecke **22**

6 Démonstration **25**

Bibliographie **27**

1 Introduction

Notons Γ le *groupe modulaire* $\Gamma(1) := \mathrm{PSL}(2, \mathbf{Z})$ quotient de $\mathrm{SL}(2, \mathbf{Z})$ par son centre $\{+\mathrm{Id}; -\mathrm{Id}\}$. Ce groupe agit à gauche, par homographies, sur le *demi-plan de Poincaré* $\mathfrak{H} := \{z \in \mathbf{C} | \Im(z) > 0\}$:

$$\pm\begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ applique } \tau \text{ sur } \frac{a \cdot \tau + b}{c \cdot \tau + d}.$$

On s'intéresse à l'espace quotient $\Gamma\backslash\mathfrak{H}$, que l'on munit naturellement de l'unique structure de surface de Riemann faisant de l'application $\mathfrak{H} \to \Gamma\backslash\mathfrak{H}$ un revêtement holomorphe, ramifié au-dessus des deux points que sont la classe de i et celle de la racine cubique de l'unité $(1 + i\sqrt{3})/2$.

Ce revêtement se décrit ainsi: la fonction modulaire j sur $\mathfrak{H}$ est donnée par la série de Laurent à coefficients entiers bien connue ([21], VII.§3.3)

$$j(\tau) = \frac{1}{q} + 744 + 196884 \cdot q + \ldots, \text{ où } q = \exp(2\pi i \tau),$$

de rayon de convergence 1 en q. Cette fonction est invariante sous l'action de Γ et induit un biholomorphisme

$$\Gamma\backslash\mathfrak{H} \xrightarrow{\sim} \mathbf{C}.$$

La fonction j fait ainsi de $\mathfrak{H}$ un revêtement holomorphe de $\mathbf{C}$, galoisien de groupe Γ et à ramification double au dessus de $j = 1728$ et triple au dessus de $j = 0$.

L'interprétation suivante en termes de courbes elliptiques est bien connue: à tout point τ de $\mathfrak{H}$ on associe le réseau $\mathbf{Z} + \tau\mathbf{Z}$ de $\mathbf{C}$ ainsi que le tore quotient $E_\tau := \mathbf{C}/(\mathbf{Z}+\tau\mathbf{Z})$. Ce dernier est une *courbe elliptique* complexe. La classe d'isomorphisme de E_τ est déterminée par un module, son *j-invariant* $j_{E_\tau} \in \mathbf{C}$ ([23], III.§1, Prop. 1.4(c)). Par exemple, la courbe elliptique complexe E donnée par l'*équation de Weierstraß* homogène[1]

$$E : Y^2Z = X^3 + aXZ^2 + bZ^3, \text{ avec } a, b \in \mathbf{C} \text{ fixés},$$

[1] On convient alors de choisir comme origine de la loi de groupe sur E le point «à l'infini», de coordonnées homogènes $[X : Y : Z] = [0 : 1 : 0]$.

a comme module $j(E) = 1728(4a)^3/16(4a^3 + 27b^2)$. En fait cet exemple est exhaustif: toute courbe elliptique complexe est isomorphe à une courbe du type précédent ([23], III.§3, Prop. 3.1). Dans le cas des courbes E_τ, il s'agit de l'équation

$$Y^2Z = 4X^3 + 60G_4(\tau)XZ^2 + 140G_6(\tau)Z^3$$

dont les coefficients s'obtiennent à partir des séries d'Eisenstein G_4 et G_6. De la sorte l'uniformisation de $E(\mathbf{C})$ s'obtient ([23], VI.§4, Prop. 3.6) au moyen de la fonction $\wp(z;\tau)$ de Weierstraß, et de sa dérivée $\wp'(z;\tau)$ en la variable z, par la formule

$$\begin{array}{ccc} \mathbf{C} & \to & E(\mathbf{C}) \\ z & \mapsto & [\wp(z;\tau) : \wp'(z;\tau) : 1]. \end{array}$$

Le résultat principal de ce texte relie deux constructions naturelles sur $\Gamma\backslash\mathfrak{H}$:

1. D'une part il existe sur $\mathfrak{H}$ une mesure borélienne invariante par homographies, unique à une constante multiplicative près. On choisit usuellement la *mesure de Poincaré*, donnée par la forme volume

$$y^{-2} \cdot \mathrm{d}x \wedge \mathrm{d}y = i/\Im(\tau)^2 \cdot \mathrm{d}\tau \wedge \mathrm{d}\bar{\tau}.$$

   On en déduit une mesure localement finie $\tilde{\mu}$ sur la base du revêtement $\Gamma\backslash\mathfrak{H}$. C'est une mesure de masse finie: $\mathrm{Vol}(\Gamma\backslash\mathfrak{H}) = \pi/3$ ([22], Théorème 2.20). On lui préférera la probabilité $\mu := \widetilde{\mu}/(\pi/3)$, que l'on nommera *probabilité hyperbolique*[2].

2. D'autre part la droite affine sur $\mathbf{C}$ est une *variété algébrique* définie sur $\mathbf{Q}$. En particulier on peut considérer l'action à gauche de $\boldsymbol{\mathcal{G}al}(\mathbf{C}/\mathbf{Q})$ sur les j-invariants de courbes elliptiques. Explicitement, étant donné un automorphisme σ de $\mathbf{C}$, si

$$j = 1728(4a)^3/16(4a^3 + 27b^2)$$

   est l'invariant j de la courbe elliptique E d'équation $Y^2 = X^3 + aX + b$, alors

$$\sigma(j) = 1728(4\sigma(a))^3/16(4\sigma(a)^3 + 27\sigma(b)^2)$$

   est, quant à lui, celui de la courbe E^σ d'équation $Y^2 = X^3 + \sigma(a)X + \sigma(b)$.

[2] L'image directe de cette probabilité sur $\mathbf{C}$, induite par la fonction j, est une probabilité à densité sur $\mathbf{C}$, que l'on notera aussi μ; elle est donnée par une forme volume à coefficients analytiques, sauf peut-être en 0 et 1728. Ces coefficients s'écrivent en terme de la fonction hypergéométrique ${}_2F_1\left(\begin{smallmatrix} 1/6 & 1/4 \\ -1/6 & 3/4 \end{smallmatrix}; j\right)$. En effet, l'inverse de la fonction j est une fonction multiforme qui se décrit en terme d'une équation différentielle Fuchsienne d'ordre 2 à deux pôles sur $\mathbf{C}$, *l'équation (hypergéométrique) de Picard-Fuchs* ([27]).

Toute courbe elliptique complexe E admet une équation de Weierstraß $Y^2 = X^3 + aX + b$ où l'on a choisi a et b dans le sous-corps $\mathbf{Q}(j(E))$ de $\mathbf{C}$ ([23], III.§1, Prop. 1.4). Réciproquement si E est donnée par une équation à coefficients dans un corps K, alors $j(E) \in K$. Par conséquent, étant donnés un corps L inclus dans $\mathbf{C}$, et une courbe elliptique complexe E admettant des équations à coefficients algébriques sur L, l'invariant $j(E)$ est algébrique sur L; autrement dit $j(E)$ n'admet qu'une orbite finie sous l'action de $\boldsymbol{\mathcal{G}al}(\mathbf{C}/L)$. On considère alors l'unique probabilité atomique sur $\mathbf{C}$ supportée par l'orbite de $j(E)$ et invariante par $\boldsymbol{\mathcal{G}al}(\mathbf{C}/L)$; on la note $\delta_L(j(E))$.

Le résultat principal de ce texte, dans le cas de l'espace $\Gamma\backslash\mathfrak{H}$, affirme que dans certaines situations on retrouve la probabilité hyperbolique μ comme limite de probabilités atomiques de la forme $\delta_L(j(E))$. Plus précisément

Théorème 1.1. *Soit L un corps de* type fini *contenu dans $\mathbf{C}$.*

Étant donnée une suite $(E_n)_{n\in\mathbf{N}}$ de courbes elliptiques complexes définies par des équations à coefficients algébriques sur L, supposées deux à deux non isomorphes*,* sans multiplication complexe*, et* mutuellement isogènes*, la probabilité $\delta_L(j(E_n))$ converge vers la probabilité hyperbolique μ lorsque n tend vers $+\infty$.*

Autrement dit, pour toute fonction continue bornée $f : \mathbf{C} \to \mathbf{R}$,

$$\delta_L(j(E_n))(f) := \frac{1}{\#\boldsymbol{\mathcal{G}al}(\mathbf{C}/L)\cdot j(E_n)} \sum_{z\in\boldsymbol{\mathcal{G}al}(\mathbf{C}/L)\cdot j(E_n)} f(z) \to \mu(f) := \int_{\mathbf{C}} f\, d\mu$$

lorsque $n \to +\infty$.

En termes imagés, la suite des orbites de $j(E_n)$ sous $\boldsymbol{\mathcal{G}al}(\mathbf{C}/L)$ *s'équidistribue pour* la probabilité μ lorsque n tend vers $+\infty$.

Dans l'énoncé 1.1, l'hypothèse que les courbes considérées proviennent d'une même classe d'isogénie est indispensable. Ne considérons que le cas où $L = \mathbf{Q}$. Les orbites sous $\boldsymbol{\mathcal{G}al}(\bar{\mathbf{Q}}/\mathbf{Q})$ de nombres algébriques n'ont pas, en général, la propriété d'équidistribution énoncée, même si tout nombre algébrique est j-invariant d'une courbe elliptique. À titre d'exemple les orbites de racines de l'unité s'équidistribuent le long du cercle unité, et une suite de singletons formés de nombres rationnels ne peut au mieux s'équidistribuer que pour une masse de Dirac, et ce uniquement si ces rationnels forment une suite de Cauchy.

William Duke a montré l'analogue du résultat précédent, pour les courbes elliptiques à multiplication complexe ([8]). Sa démonstration utilise des méthodes spectrales (bornes de sous-convexité de Burgess, d'Iwaniec, les conjectures de Weil, les formes de Maaß). Elle permet par contre de ne pas supposer que les courbes considérées soient isogènes.

Un premier fait non trivial contenu dans l'énoncé 1.1 est le corollaire suivant

Corollaire 1.2. *Pour une suite $(E_n)_{n\in\mathbf{N}}$ telle que dans le théorème, le degré $[L(j(E_n)) : L]$ tend vers $+\infty$ lorsque n tend vers $+\infty$. En particulier, sur un*

corps K de type fini sur $\mathbf{Q}$ fixé, il n'y a qu'un nombre fini de courbes elliptiques $\mathbf{C}$-isogènes à une courbe donnée, comptées à $\mathbf{C}$-isomorphisme près.

Si $j(E_i)$ est transcendant pour un indice i, il en est de même pour chaque indice. Pour un tel cas[3], le corollaire se déduit des résultats de Shimura et Hecke. Pour tout $N \in \mathbf{N}_{>0}$, soit $\Phi_N(X,Y)$ le polynôme modulaire d'ordre N tel que construit dans [24], Exercice 2.18. C'est un polynôme à coefficients entiers (2.18 (a)), irréductible en la variable Y au dessus de $\mathbf{C}(X)$ et de degré $\#\mathbf{P}_1(\mathbf{Z}/(N))$ en chacune de ses variables (2.17 (b) et 2.18(c)). Spécialisons X en $j(E_i)$. Dès lors $\Phi_N(X,Y)$ se spécialise en un polynôme dont les racines sont les j-invariants des courbes elliptiques complexes reliées à E_i par une isogénie *cyclique* d'ordre N (2.19 (b)). Comme $j(E_i)$ est transcendant sur $\mathbf{Q}$, cette spécialisation induit un isomorphisme $\mathbf{Q}(X) \xrightarrow{\sim} \mathbf{Q}(j(E_i))$. Comme $\Phi_N(X,Y)$ est irréductible sur $\mathbf{C}(X)$, donc aussi sur $\mathbf{Q}(X)$, le polynôme $\Phi_N(j(E_i),Y)$ est irréductible sur $\mathbf{Q}(j(E_i))$. Autrement dit les nombres $j(E)$ tels que E est reliée à E_i par une isogénie cyclique de degré N sont conjugués sous $\boldsymbol{\mathcal{G}al}(\mathbf{C}/\mathbf{Q}(j(E_i))$ et sont de degré $\#\mathbf{P}_1(\mathbf{Z}/(N))$ sur $\mathbf{Q}(j(E_i))$. En particulier il n'y a qu'un nombre fini, à isomorphisme près, de telles courbes E. Comme les E_n sont deux à deux non isomorphes, le degré N_n d'une isogénie cyclique reliant E_n à E_i tend vers $+\infty$, de même que le degré $[\mathbf{Q}(j(E_n)) : \mathbf{Q}] = \#\mathbf{P}_1(\mathbf{Z}/(N_n))$. Il suit, étant donné un corps L de type fini sur $\mathbf{Q}$, que $[L(j(E_n)) : L(j(E_i))]$ tend vers l'infini avec n.

Dans le cas de courbes définissables sur des corps de nombres, il est possible que l'on puisse déduire ce corollaire du théorème de Šafarevič (cf. [19], page IV 7, où l'on considère des courbes mutuellement K-isogènes comptées à K-isomorphisme près) et du *théorème de finitude de Faltings* ([10], sous la forme du Corollaire 2.8 de [6]). On préférera déduire cette propriété du théorème *de l'image ouverte de Serre* et de théorèmes généraux d'Armand Borel sur les groupes arithmétiques. Ce sera l'objet de la partie 4. On aura l'occasion d'établir en passant divers énoncés de finitude sur les groupes arithmétiques et adéliques dont certains seront réutilisés par la suite. Cette méthode redémontre aussi le corollaire dans le cas transcendant, en substituant au théorème de l'image ouverte son analogue (Proposition 3.5).

Remarquons enfin que la notion de convergence utilisée dans l'énoncé est la *convergence étroite*. En particulier il n'y a pas de «perte de masse à l'infini». Ceci est d'autant plus remarquable que dans une même classe d'isogénie, la *hauteur* de j-invariants deux à deux distincts n'est en général pas bornée ([25]).

Avant de continuer, esquissons ici les étapes principales de la démonstration. Le point de départ est le théorème de l'image ouverte de Jean-Pierre Serre, qui nous permet de comprendre les orbites du groupe de Galois sur

[3]Le nombre complexe $j(E_i)$ définit alors un *point générique*, dans le langage de Weil, de la droite affine sur $\mathbf{Q}$. Or $\mathrm{Aut}(\mathbf{C})$ permute transitivement l'ensemble de ces points. D'un point de vue algébrique, il suffira de ne considérer que le point générique du schéma associé.

la courbe modulaire en termes d'actions du groupe adélique $\mathrm{GL}(2,\hat{\mathbf{Z}})$ dans l'espace $\mathrm{PGL}(2,\mathbf{Q})\backslash\mathrm{PGL}(2,\mathbf{A})/\mathrm{PGL}(2,\hat{\mathbf{Z}})$. Quitte à identifier cet espace avec $\mathrm{PGL}(2,\mathbf{Z})\backslash\mathrm{PGL}(2,\mathbf{R})$, notre problème se ramène à étudier des «orbites de Hecke» au sens de [9]. Ce dernier problème est résolu dans [9] en se basant sur des méthodes ergodiques issues des théorèmes de Ratner[4]. Pour appliquer [9], il faut toutefois vérifier que le cardinal des orbites considérées tend vers $+\infty$. L'énoncé 1.2 nous apprend que cette hypothèse est automatiquement vérifiée dans le cadre arithmétique dans lequel nous nous plaçons. Pour démontrer 1.2, nous nous basons sur des théorèmes d'A. Borel. Enfin, pour terminer la démonstration, il nous faut vérifier que le résultat d'équidistribution dans $\mathrm{PGL}(2,\mathbf{Z})\backslash\mathrm{PGL}(2,\mathbf{R})$ obtenu à partir de [9] redonne bien le résultat cherché sur la courbe modulaire.

Nous avons pris le souci d'utiliser des arguments qui s'appliquent au cas de variétés de Shimura plus générales que les courbes modulaires, comme les espaces de modules de variétés abéliennes. L'auteur remercie un rapporteur qui lui a fait remarquer que, dans ce contexte plus général, la généralisation de notre théorème répond à une question de R. Pink (Remarque 7.7(b) de [17]) en la précisant. Mais, dans ce cadre, notre méthode nécessite d'admettre comme hypothèse l'analogue du théorème de l'image ouverte de Serre, qui est une forme renforcée de la *conjecture de Mumford-Tate*. Or cette dernière n'est pas démontré dans certains cas, à commencer par la dimension 4. Un article en préparation démontre, sous forme conditionnelle, une telle généralisation. Pour les variétés de Shimura de type abélien, il semblerait que les résultats de [10] suffisent pour obtenir variante légèrement affaiblie, mais inconditionnelle.

Je remercie Pascal Autissier, Bachir Bekka, Serge Cantat, Antoine Chambert-Loir, Antoine Ducros, Bas Edixhoven, Yves Guivarc'h, Franck Loray, Laurent Moret-Bailly et Nimish Shah pour leur influence sur ce travail, que ce soit leurs encouragements, leur disponibilité, leur patience, leurs enseignements, les discussions que nous avons eues *etc.* et leur bonne humeur. Je remercie également l'École Normale et l'IRMAR pour les conditions dans lesquelles il m'a été permis de mener à bien ce travail.

Nous allons à présent énoncer, en toute généralité, le résultat principal de ce texte. C'est à cette fin que nous commencerons par quelques rappels sur les courbes modulaires de niveau N.

[4]En ce qui concerne les théorèmes 1.1 et 2.1, on peut ne faire usage que du cas particulier $G = \mathrm{SL}(2,\mathbf{R})$, $\Gamma = \mathrm{SL}(2,\mathbf{Z})$ de [9]. Il n'apparaît peut-être pas clairement dans [9] qu'il suffit d'appliquer le théorème de Ratner qu'au groupe G (et pas nécessairement $G \times G$). En tout état de cause il semble, selon [9], que ce «classical case [...] [was] known for a long time».

2 Courbes $Y(N)$, Action galoisienne et Énoncé

Soit N un entier naturel non nul. On note ζ_N la racine primitive N-ième de l'unité $\exp(2\pi i/N)$ de $\mathbf{C}$. Rappelons que $\Gamma(N) \triangleleft \Gamma(1)$ désigne le N-ième sous-groupe principal de congruence, image dans $\mathrm{PSL}(2,\mathbf{Z})$ du noyau du morphisme de réduction modulo (N) : $\mathrm{SL}(2,\mathbf{Z}) \to \mathrm{SL}(2,\mathbf{Z}/(N))$.

Notons $E[N]$ le sous-groupe des points de N-torsion d'une courbe elliptique complexe E. C'est un groupe isomorphe à $(\mathbf{Z}/(N))^2$. Se donner une *structure complète de niveau* N sur une courbe elliptique complexe E, c'est choisir un isomorphisme β entre $(\mathbf{Z}/(N))^2$ et le sous-groupe $E[N]$ des points de N-torsion de E; cela revient aussi à se donner une $\mathbf{Z}/(N)$-base $(P_1, P_2) = \beta((1,0),(0,1))$ de la N-torsion de E.

L'*accouplement de Weil* de E définit une forme bilinéaire alternée non dégénérée canonique $e_N : E[N] \times E[N] \to \boldsymbol{\mu}_N$ à valeur dans le groupe $\boldsymbol{\mu}_N$ des racines N-ièmes de l'unité. Nous conviendrons d'utiliser la normalisation de [13], 18 §1 App. Cette normalisation est aussi compatible avec la définition de [24] (cf. Exercice 1.15), qui reprend la construction de [22].

Pour tout point τ de $\mathfrak{H}$, la courbe elliptique $E_\tau = \mathbf{C}/(\mathbf{Z} + \tau\mathbf{Z})$ porte une structure $\beta(\tau)$ de niveau N canonique: en effet la N-torsion de E_τ est engendrée par les images $P_1(\tau)$ et $P_2(\tau)$ des deux points $1/N$ et τ/N de $\mathbf{C}$. On en déduit une racine primitive de l'unité $\zeta(\tau) = e_N(P_1(\tau), P_2(\tau))$ canoniquement associée à τ. Par calcul, on trouve $\zeta(\tau) = \zeta_N$ pour tout τ dans $\mathfrak{H}$ ([13], 18 §1 App., ou [24], Exercice 1.15).

On vérifie que deux points τ et τ' de $\mathfrak{H}$ donnent lieu à deux courbes $(E_\tau, \beta(\tau))$ et $(E_{\tau'}, \beta(\tau'))$ avec structure de niveau N isomorphes si et seulement si $\tau = \gamma \cdot \tau'$ avec $\gamma \in \Gamma(N)$. En fait $\Gamma(N)\backslash\mathfrak{H}$ paramètre ainsi *toutes* les classes d'isomorphisme de courbes elliptiques munies d'une structure complète de niveau N dont la racine de l'unité associée est ζ_N. Pour $k \in \mathbf{Z}/(N)^\star$, on obtient les structures de niveau de racine de l'unité associée ${\zeta_N}^k$, en considérant, au choix, les bases du type $(k/N, \tau/N)$ ou $(1/N, k\tau/N)$.

Dans le cas $N = 1$, $\Gamma(N)\backslash\mathfrak{H}$ s'identifie à l'ensemble $\mathbf{A}^1(\mathbf{C})$ des points complexes de la droite affine $\mathbf{A}^1$. De façon analogue, la courbe modulaire $Y(N)$ est une courbe algébrique (affine et *géométriquement connexe*) sur $\mathbf{Q}(\zeta_N)$ qui «paramètre[5]» les courbes elliptiques munies d'une structure complète de niveau N dont la racine associée est ζ_N. L'espace analytique $Y(N)(\mathbf{C})$ formé de ses points complexes s'identifie ainsi avec la surface de Riemann $\Gamma(N)\backslash\mathfrak{H}$. Pour $N = 1$, on retrouve le biholomorphisme $\Gamma\backslash\mathfrak{H} \xrightarrow{\sim} \mathbf{A}^1(\mathbf{C})$ induit par la fonction j. L'espace $\Gamma(N)\backslash\mathfrak{H}$ porte donc une probabilité hyperbolique canonique, notée μ, ainsi qu'une action du groupe $\boldsymbol{\mathcal{G}al}(\mathbf{C}/\mathbf{Q}(\zeta_N))$.

[5] *Stricto sensu* il s'agit d'un espace de module grossier pour $N = 1$ ou 2, et fin pour $N \geq 3$, du problème de classification associé. On peut par exemple prendre la fibre générique des $\mathtt{Spec}(\mathbf{Z}[1/N, \zeta_N])$-schémas construits dans [7] ou [12].

La probabilité μ se construit comme dans le cas de $\Gamma\backslash\mathfrak{H}$ détaillé en introduction. L'action de $\boldsymbol{\mathcal{G}al}(\mathbf{C}/\mathbf{Q}(\zeta_N))$ se décrit ainsi: Soit $\sigma \in \boldsymbol{\mathcal{G}al}(\mathbf{C}/\mathbf{Q}(\zeta_N))$ et soit $z \in Y(N)(\mathbf{C})$. Alors x peut être représenté par une une courbe elliptique complexe E donnée par une équation de Weierstraß $Y^2Z = X^3 + aXZ^2 + bZ^3$ et munie d'une base $(P_1 = [X_1 : Y_1 : Z_1], P_2 = [X_2 : Y_2 : Z_2])$ de la N-torsion. Dès lors le point $\sigma(z)$ est représenté par la courbe E^σ donnée par $Y^2Z = X^3 + \sigma(a)XZ^2 + \sigma(b)Z^3$ et munie de la base $({P_1}^\sigma = [\sigma(X_1) : \sigma(Y_1) : \sigma(Z_1)], {P_2}^\sigma = [\sigma(X_2) : \sigma(Y_2) : \sigma(Z_2)])$. On vérifie qu'à cette dernière on associe la racine $e_N({P_1}^\sigma, {P_2}^\sigma) = \sigma(e_N(P_1, P_2)) = \sigma(\zeta_N) = \zeta_N$, puisque σ agit comme l'identité sur $\mathbf{Q}(\zeta_N)$.

Soit L un corps de type fini contenu dans $\mathbf{C}$ et contenant $\mathbf{Q}(\zeta_N)$. Soit $z \in Y(N)(\mathbf{C})$ un point complexe supposé *algébrique sur* L. Alors l'orbite de z sous $\boldsymbol{\mathcal{G}al}(\mathbf{C}/L)$ est finie, et est le support d'une unique probabilité borélienne atomique $\boldsymbol{\mathcal{G}al}(\mathbf{C}/L)$-invariante, que l'on notera $\delta_L(z)$, sur $Y(N)(\mathbf{C})$.

Le résultat principal de ce texte est une généralisation de l'énoncé 1.1 au cas des structures complètes de niveau N. Il permet, sur la surface de Riemann $Y(N)(\mathbf{C})$, d'obtenir la mesure hyperbolique μ comme limite étroite de probabilités atomiques du type $\delta_L(z)$. Plus précisément

Théorème 2.1. *Soit L un corps* de type fini *contenu dans $\mathbf{C}$ et contenant $\mathbf{Q}(\zeta_N)$.*

Soit $z_n \in Y(N)(\mathbf{C})$ une suite de points deux à deux distincts. *Supposons que les z_n sont représentés par des structures complètes de niveau N sur des courbes elliptiques complexes E_n* deux à deux isogènes *et* sans multiplication complexe *définies par des équations à coefficients algébriques sur L.*

Alors $\delta_L(z_n)$ converge vers μ lorsque n tend vers $+\infty$.

Autrement dit, pour toute fonction continue bornée $f : Y(N)(\mathbf{C}) \to \mathbf{R}$,

$$\delta_n(f) := \frac{1}{\#\boldsymbol{\mathcal{G}al}(\mathbf{C}/L)\cdot z_n} \sum_{z\in\boldsymbol{\mathcal{G}al}(\mathbf{C}/L)\cdot z_n} f(z) \to \mu(f) := \int_{Y(N)(\mathbf{C})} f\, d\mu$$

lorsque $n \to +\infty$.

On dira que la suite des orbites de x_n sous $\boldsymbol{\mathcal{G}al}(\mathbf{C}/L)$ *s'équidistribue pour* la probabilité μ.

Le théorème 1.1 est un cas particulier de l'énoncé précédent pour $N = 1$, modulo l'identification $Y(1)(\mathbf{C}) \simeq \Gamma(1)\backslash\mathfrak{H} \xrightarrow{\sim} \mathbf{C}$.

Soit $\bar{L}$ la fermeture algébrique de L dans $\mathbf{C}$. Le fait que E_n soit définie sur $\bar{L}$ équivaut à ce que z_n appartienne au sous-ensemble $Y(N)(\bar{L})$ de $Y(N)(\mathbf{C})$. Cela revient aussi à dire que $j(E_n) \in \bar{L}$. Les probabilités $\delta_L(z_n)$ sont donc bien définies. Comme les E_n sont deux à deux isogènes, il suffit même de supposer que z_n n'appartient à $Y(N)(\bar{L})$, voire que $j(E_n) \in \bar{L}$, et ce pour une seule valeur de l'indice n ([23], III.§4).

3 Action galoisienne sur une classe d'isogénie

Dans cette section nous décrivons sous une forme plus commode la classe d'isogénie d'une courbe elliptique complexe (cf. Proposition 3.1). De plus, dans le cas d'une courbe définissable sur un corps L de type fini, nous explicitons l'action de $\boldsymbol{\mathcal{G}al}(\mathbf{C}/L)$ sur sa classe d'isogénie (Proposition 3.3). Enfin nous expliciterons comment relier les ensembles que nous aurons obtenus avec les courbes modulaires introduites précédemment (Proposition 3.6). Ce sont des propriétés bien connues et le seul point difficile, identifier l'action galoisienne dans le cas algébrique, sera en fait un corollaire du théorème de l'image ouverte de Serre.

Rappelons brièvement que $\hat{\mathbf{Z}}$ désigne le complété de $\mathbf{Z}$ pour la base de voisinages de 0 donnée par les idéaux non nuls de $\mathbf{Z}$, c'est-à-dire ses sous-groupes additifs d'indice fini: On a $\hat{\mathbf{Z}} = \varprojlim_{N\in(\mathbf{N}_{>0},\times)} \mathbf{Z}/(N)$. C'est un anneau profini, donc compact et totalement discontinu; il contient $\mathbf{Z}$ comme sous-anneau dense. On tire du lemme chinois la décomposition $\hat{\mathbf{Z}} = \prod_{p \text{ premier}} \mathbf{Z}_p$ en terme d'anneaux d'entiers p-adiques. On forme l'anneau $\mathbf{A}_f \simeq \hat{\mathbf{Z}}\otimes_{\mathbf{Z}}\mathbf{Q}$ des adèles aux places finies, où l'on considère la topologie discrète sur $\mathbf{Q}$ et $\mathbf{Z}$. C'est un anneau localement compact constitué des suites $(n_p/m_p)_{p \text{ premier}}$ de $\prod_{p \text{ premier}} \mathbf{Q}_p$ n'admettant un dénominateur que pour au plus un nombre fini d'indices. Enfin $\mathbf{A} \simeq \mathbf{R} \times \mathbf{A}_f$ désigne l'anneau des adèles. Il est lui aussi localement compact; en outre $\mathbf{Q}$ se plonge, de façon diagonale, sur un sous-anneau *discret* et *cocompact* de celui-ci.

Nous introduisons la notation suivante, où G est un groupe algébrique linéaire sur $\mathbf{Q}$ pour lequel la formule $G(\mathbf{Z})$ a un sens, par exemple lorsque G est un sous groupe de $\mathrm{GL}(n)$: On désignera par $G[N\mathbf{Z}]$ (respectivement $G[N\hat{\mathbf{Z}}]$) le noyau du morphisme réduction modulo $N\mathbf{Z}$ (resp. $N\hat{\mathbf{Z}}$) $G(\mathbf{Z}) \to G(\mathbf{Z}/N\mathbf{Z})$ (resp. $G(\hat{\mathbf{Z}}) \to G(\mathbf{Z}/N\mathbf{Z})$); c'est le sous-groupe de $G(\mathbf{Z})$ (resp. $G(\hat{\mathbf{Z}})$) des matrices congrues à l'identité modulo (N).

Voici le premier des énoncés que nous allons démontrer

Proposition 3.1. *Soit E une courbe elliptique complexe* sans multiplication complexe*, et soit $\beta : (\mathbf{Z}/(N))^2 \xrightarrow{\sim} E[N]$ une structure complète de niveau N sur E de racine de l'unité associée égale à ζ_N. On se fixe également, pour simplifier, une base de $\hat{T}(E)$ relevant β.*

1. *Alors les classes d'isomorphisme de courbes elliptiques complexes E' isogènes à E munies d'une structure complète β' de niveau N forment un ensemble* $\mathrm{Isog}_N(E)$ *qui s'identifie naturellement à*

$$\mathbf{Q}^\star\backslash\mathrm{Isom}({\mathbf{A}_f}^2, \hat{V}(E))/\mathrm{GL}(2)[N\hat{\mathbf{Z}}],$$

c'est-à-dire, étant donné que l'on s'est choisi une base de $\hat{T}(E)$*, à*

$$\mathbf{Q}^\star\backslash \mathrm{GL}(2,\mathbf{A}_f)/\mathrm{GL}(2)[N\hat{\mathbf{Z}}]$$

ou même, compte tenu du théorème d'approximation forte, à

$$\mathbf{Q}^\star\backslash \mathrm{GL}(2,\mathbf{Q})\mathrm{GL}(2,\hat{\mathbf{Z}})/\mathrm{GL}(2)[N\hat{\mathbf{Z}}].$$

2. *En outre, l'application qui fait correspondre à la classe du couple* (E,β') *la racine primitive* N*-ième associée s'identifie alors à l'application*

$$\begin{array}{ccc} \mathbf{Q}^\star\backslash \mathrm{GL}(2,\mathbf{Q})\mathrm{GL}(2,\hat{\mathbf{Z}})/\mathrm{GL}(2)[N\hat{\mathbf{Z}}] & \longrightarrow & \mu_N(\mathbf{C}), \\ \mathbf{Q}^\star\cdot(q\cdot z)\cdot\mathrm{GL}(2)[N\hat{\mathbf{Z}}] & \longmapsto & (\zeta_N)^{\mathbf{dét}(z)}. \end{array}$$

3. *Désignons par* $\mathrm{Isog}_{N,\zeta_N}(E)$ *le sous-ensemble des points de* $Y(N)(\mathbf{C})$ *qui sont représentés par une structure de niveau* N *de racine associée* ζ_N *sur une courbe elliptique complexe isogène à* E*.*

   Alors $\mathrm{Isog}_{N,\zeta_N}(E)$ *s'identifie au sous-ensemble de* $\mathrm{Isog}_N(E)$ *induit par*

$$\mathbf{Q}^\star\backslash \mathrm{GL}(2,\mathbf{Q})\mathrm{GL}(2)[N\hat{\mathbf{Z}}]/\mathrm{GL}(2)[N\hat{\mathbf{Z}}].$$

Quelques remarques avant de poursuivre. Tout d'abord les actions des deux groupes $\mathrm{Aut}({\mathbf{A}_f}^2)$ et $\mathrm{Aut}(\hat{V}(E))$ sur $\mathrm{Isom}({\mathbf{A}_f}^2,\hat{V}(E))$ se font par composition, à droite pour $\mathrm{Aut}({\mathbf{A}_f}^2)$ et à gauche quant à $\mathrm{Aut}(\hat{V}(E))$; ce sont donc des actions *à droite* et *à gauche* respectivement[6]. En ce qui concerne second point de la conclusion, il faut savoir que tout élément g de $\mathrm{GL}(2,\mathbf{A}_f)$ peut se mettre sous la forme $q\cdot z$ avec $q\in\mathrm{GL}(2,\mathbf{Q})$ et $z\in\mathrm{GL}(2,\hat{\mathbf{Z}})$ ([11], page 66).

Nous nous inspirons de l'exposition de [7], page 75: Soit k un corps algébriquement clos de caractéristique 0; seuls nous importeront les cas où k est $\mathbf{C}$, $\bar{\mathbf{Q}}$ ou plus généralement la fermeture algébrique dans $\mathbf{C}$ du corps L de type fini considéré dans 2.1. On considère la catégorie $\mathbf{Q}$-linéaire $\mathcal{E}\ell\ell(k)\otimes\mathbf{Q}$ des «courbes elliptiques à isogénie près» sur k définie ainsi:

- Les catégories $\mathcal{E}\ell\ell(k)$ et $\mathcal{E}\ell\ell(k)\otimes\mathbf{Q}$ ont les mêmes objets. On notera toutefois $E\otimes\mathbf{Q}$ la «courbe elliptique à isogénie près» induite par E.
- Les flèches de $\mathcal{E}\ell\ell(k)\otimes\mathbf{Q}$ (et leur composition) sont données par la formule

$$\mathrm{Hom}(E\otimes\mathbf{Q},F\otimes\mathbf{Q}) := \mathrm{Hom}(E,F)\otimes_{\mathbf{Z}}\mathbf{Q}.$$

[6] La convention que nous utilisons pour la latéralisation des actions de groupe est opposée à celle des *Éléments de mathématique* de N. Bourbaki: nous nommerons un élément gH de G/H une classe *à droite*.

En particulier $E \otimes \mathbf{Q}$ est isomorphe à $F \otimes \mathbf{Q}$ signifie que E et F sont isogènes.

La considération du module de Tate induit un foncteur additif

$$[f : E \to F] \mapsto [\hat{T}(f) : \hat{T}(E) \to \hat{T}(F)]$$

de $\mathcal{E}\ell\ell(k)$ vers la catégorie $\mathcal{M}od_{\hat{\mathbf{Z}}}$ des $\hat{\mathbf{Z}}$ modules. Celui-ci induit aussi un foncteur $[f : E \otimes \mathbf{Q} \to F \otimes \mathbf{Q}] \mapsto [\hat{V}(f) : \hat{V}(E \otimes \mathbf{Q}) \to \hat{V}(F \otimes \mathbf{Q})]$ de $\mathcal{E}\ell\ell(k) \otimes \mathbf{Q}$ vers $\mathcal{M}od_{\mathbf{A}_f}$. On retrouve alors $\mathrm{Hom}_{\mathcal{E}\ell\ell(k)}(E, F)$ comme le sous-ensemble des morphismes $f \in \mathrm{Hom}(E \otimes \mathbf{Q}, F \otimes \mathbf{Q})$ tels que $\hat{V}(f)(\hat{T}(E)) \subseteq \hat{T}(F)$.

Soit $\hat{V}$ un $\mathbf{A}_f$-module libre de rang 2. Un *réseau* de $\hat{V}$ désignera ici un sous-groupe compact ouvert $\hat{T}$ de celui-ci. La donnée de $\hat{T}$ équivaut à celle d'une $\mathrm{GL}(2, \hat{\mathbf{Z}})$-classe à droite d'isomorphismes $\mathbf{A}_f$-linéaires du plan ${\mathbf{A}_f}^2$ avec $\hat{V}$: à la classe

$$B \in \mathrm{Isom}({\mathbf{A}_f}^2, \hat{V})/\mathrm{GL}(2, \hat{\mathbf{Z}})$$

correspond le réseau $\beta(\hat{\mathbf{Z}}^2)$, où $\beta : {\mathbf{A}_f}^2 \xrightarrow{\sim} \hat{V}$ désigne n'importe quel isomorphisme de classe B. En outre, le choix de l'une des $\mathrm{GL}(2)[N\hat{\mathbf{Z}}]$-classes contenues dans B

$$C \in B/\mathrm{GL}(2)[N\hat{\mathbf{Z}}] \subseteq \mathrm{Isom}({\mathbf{A}_f}^2, \hat{V})/\mathrm{GL}(2)[N\hat{\mathbf{Z}}],$$

revient à choisir un isomorphisme de $(\mathbf{Z}/(N))^2 \simeq \hat{\mathbf{Z}}^2 \otimes \mathbf{Z}/(N)$ avec $\varphi(\hat{\mathbf{Z}}^2) \otimes \mathbf{Z}/(N)$: celui induit par $\beta \otimes \mathbf{Z}/(N)$, peu importe $\beta \in C$.

On définit ensuite la catégorie $\mathcal{E}\ell\ell(k)'$ des couples $(E \otimes \mathbf{Q}, B)$, où B est un réseau de $\hat{V}(E \otimes \mathbf{Q})$, pour laquelle

$$\mathrm{Hom}((E \otimes \mathbf{Q}, B), (F \otimes \mathbf{Q}, C)) \subseteq \mathrm{Hom}(E \otimes \mathbf{Q}, F \otimes \mathbf{Q})$$

est défini par $\hat{V}(f)(\beta(\hat{\mathbf{Z}}^2)) \subseteq \gamma(\hat{\mathbf{Z}}^2)$, pour $\beta \in B$ et $\gamma \in C$. Il est immédiat que l'on obtient ainsi une catégorie équivalente à $\mathcal{E}\ell\ell(k)$, une équivalence étant celle qui associe à la courbe elliptique E le couple $(E \otimes \mathbf{Q}, \hat{T}(E))$. De plus tout objet $(E' \otimes \mathbf{Q}, B)$ de $\mathcal{E}\ell\ell(k)'$ tel que E' est isogène à E, est isomorphe à $(E \otimes \mathbf{Q}, B')$ pour un B' convenable, par exemple $\hat{V}(f)_\star B$, pour f choisi dans $\mathrm{Isom}(E' \otimes \mathbf{Q}, E \otimes \mathbf{Q})$.

On définit enfin le groupoïde $\mathcal{E}\ell\ell_N(k)$, comme la catégorie dont les objets sont les couples $(E \otimes \mathbf{Q}, B)$ où $B \in \mathrm{Isom}(\hat{V}(E), {\mathbf{A}_f}^2)/\mathrm{GL}(2)[N\hat{\mathbf{Z}}]$ et ayant comme isomorphismes de $(E \otimes \mathbf{Q}, B)$ vers $(F \otimes \mathbf{Q}, C)$ les isomorphismes f dans $\mathrm{Isom}(E \otimes \mathbf{Q}, F \otimes \mathbf{Q})$ tels que $B = f^\star C$. Le groupoïde $\mathcal{E}\ell\ell_N(k)$ ainsi construit est équivalent à la catégorie formée des courbes elliptiques sur k avec structure complète de niveau N et des k-isomorphismes compatibles aux structures[7], pour l'équivalence qui à E munie de $\beta : (\mathbf{Z}/(N))^2 \xrightarrow{\sim} E[N]$ fait correspondre $E \otimes \mathbf{Q}$ munie de la classe d'isomorphismes de ${\mathbf{A}_f}^2$ vers $\hat{V}(E \otimes \mathbf{Q})$

[7] La considération de la famille des groupoïdes analogues aux $\mathcal{E}\ell\ell_N(k)$, pour un schéma k variable, donne en fait lieu au champ modulaire $\mathfrak{M}_N^0$ construit dans [7].

relevant β. L'ensemble Isog_N s'identifie ainsi aux classes d'isomorphismes de $\mathcal{E}\ell\ell_N(k)$.

De même que pour $\mathcal{E}\ell\ell(k)'$, toute classe d'isomorphisme dans $\mathcal{E}\ell\ell_N(k)$ qui est représentée par $(E' \otimes \mathbf{Q}, B)$, où E' est isogène à E, admet un représentant de la forme $(E \otimes \mathbf{Q}, B')$; on en déduit

Proposition 3.2. *L'ensemble* $\mathrm{Isog}_N(E)$ *des classes d'isomorphisme de* $\mathcal{E}\ell\ell_N(k)$ *représentées par un couple* (E', B) *tel que la courbe* E' *est* isogène *à* E *est en bijection naturelle avec*

$$\mathrm{Aut}(E \otimes \mathbf{Q}) \backslash \mathrm{Isom}({\mathbf{A}_f}^2, \hat{V}(E)) / \mathrm{GL}(2)[N\hat{\mathbf{Z}}],$$

où $\mathrm{End}(E \otimes \mathbf{Q})$ *agit fidèlement sur* $\hat{V}(E)$ *via le foncteur* $\hat{V}$.

On remarque que lorsque E n'admet pas de multiplication complexe le groupe $\mathrm{Aut}(E \otimes \mathbf{Q})$ est réduit à $\mathbf{Q}^\star$, et que sinon $\mathrm{Aut}(E \otimes \mathbf{Q})$ vaut $K^\star$ où K est le *corps de multiplication complexe* de E. On a ainsi démontré le premier point de la proposition 3.1.

Soit maintenant $z \in \mathrm{Isog}_N(E)$ une classe d'isomorphisme de $\mathcal{E}\ell\ell_N(k)$. On va expliciter l'action d'un élément g de $\mathrm{GL}(2, \hat{\mathbf{Z}})$ sur cette classe. À cet effet, soit E une courbe elliptique sur k munie d'une structure complète de niveau N représentant cette classe. Choisissons également β un isomorphisme de $\hat{\mathbf{Z}}^2$ vers $\hat{T}(E)$ relevant cette structure de niveau. Alors g envoie la classe de $(E, \beta \otimes \mathbf{Q} : {\mathbf{A}_f}^2 \xrightarrow{\sim} \hat{V}(E))$ sur celle de $(E, (\beta \circ g) \otimes \mathbf{Q} : {\mathbf{A}_f}^2 \xrightarrow{\sim} \hat{V}(E))$. Donc la classe $z \cdot g$, pour $g \in \mathrm{GL}(2, \hat{\mathbf{Z}})$ est représentée par la structure de niveau $(\beta \circ g) \otimes \mathbf{Z}/(N) : (\mathbf{Z}/(N))^2 \xrightarrow{\sim} E[N](k)$ sur E.

Notons $\beta_N = \beta \otimes \mathbf{Z}/(N) : (\mathbf{Z}/(N))^2 \xrightarrow{\sim} E[N](k)$ et $g_N = g \otimes \mathbf{Z}/(N) : (\mathbf{Z}/(N))^2 \xrightarrow{\sim} (\mathbf{Z}/(N))^2$. Par définition, la structure β_N sur E admet $\zeta := e_N(\beta_N(1,0), \beta_N(1,0))$ comme racine associée. La structure $(\beta \circ g) \otimes \mathbf{Z}/(N)$ quant à elle a pour racine associée $e_N(\beta_N \circ g_N(1,0), \beta_N \circ g_N(1,0))$, soit également $\zeta^{\mathbf{dét}(g)}$, e_N étant bilinéaire, alternée à valeurs dans $\mu_N(k)$. On en déduit le second point de la proposition 3.1. Le troisième point quant à lui découle de ce second point, à ceci près qu'il faut remarquer que $\mathrm{GL}(2, \mathbf{Q}) \cdot \mathrm{GL}(2)[N\hat{\mathbf{Z}}] = \mathrm{GL}(2, \mathbf{Q}) \cdot \mathrm{SL}(2, \hat{\mathbf{Z}})\mathrm{GL}(2)[N\hat{\mathbf{Z}}]$, où on reconnaît en $\mathrm{SL}(2, \hat{\mathbf{Z}})\mathrm{GL}(2)[N\hat{\mathbf{Z}}]$ le sous-groupe des matrices de $\mathrm{GL}(2, \hat{\mathbf{Z}})$ dont le déterminant est congru à 1 modulo (N). Mais cela provient du fait que l'intersection $\mathrm{SL}(2, \mathbf{Z})$ de $\mathrm{GL}(2, \mathbf{Q})$ avec $\mathrm{SL}(2, \hat{\mathbf{Z}})$ est dense dans ce dernier ([11], page 69).

On va maintenant expliciter les propriétés galoisiennes du sous-ensemble $\mathrm{Isog}_{N,\zeta_N}(E)$ de $Y(N)(\mathbf{C})$. Plus précisément on va établir l'énoncé suivant

Proposition 3.3. *Soit* L *une extension* de type fini *de* $\mathbf{Q}(\zeta_N)$ *contenue dans* $\mathbf{C}$. *Soit* E *une courbe elliptique complexe* sans multiplication complexe *munie d'une structure complète* β *de niveau* N *de racine associée* ζ_N. *Supposons que* (E, β) *admet un modèle* $(E, \beta) \xrightarrow{\sim} (E_L, \beta_L) \otimes_L \mathbf{C}$, *où* E_L *est une courbe elliptique*

définie sur L et où β_L est définie sur L. Ainsi $\mathrm{Isog}_{N,\zeta_N}(E)$ *est constitué de points de $Y(N)(\mathbf{C})$ algébriques sur L et porte une action de $\boldsymbol{\mathcal{G}al}(\mathbf{C}/L)$.*

Considérons une base de $\hat{T}(E)$ relevant β, et soit

$$\rho : \boldsymbol{\mathcal{G}al}(\mathbf{C}/L) \to \mathrm{GL}(2, \hat{\mathbf{Z}})$$

la représentation galoisienne sur le module de Tate de E associée au modèle E_L écrite dans la base que l'on s'est fixé.

Alors, d'une part, cette représentation a un conoyau fini, et d'autre part, pour tout $\sigma \in \boldsymbol{\mathcal{G}al}(\mathbf{C}/L)$, l'action de σ sur $\mathrm{Isog}_{N,\zeta_N}(E)$ *s'obtient par restriction de l'action naturelle par multiplication à gauche de $\rho(\sigma)$ sur* $\mathrm{Isog}_N(E)$.

Autrement dit l'action de $\boldsymbol{\mathcal{G}al}(\mathbf{C}/L)$ sur $\mathrm{Isog}_{N,\zeta_N}(E)$ *est isomorphe à celle d'un sous-groupe d'indice fini de* $\mathrm{GL}(2, \hat{\mathbf{Z}})$ *sur*

$$\mathbf{Q}^\star \backslash \mathrm{GL}(2, \mathbf{Q}) \mathrm{GL}(2)[N\hat{\mathbf{Z}}] / \mathrm{GL}(2)[N\hat{\mathbf{Z}}],$$

par multiplication à gauche.

Remarquons ici que, comme $\mathbf{Q}^\star$ est contenu dans le *centre* de $\mathrm{GL}(2, \mathbf{A}_f)$, l'action à gauche de $\mathrm{GL}(2, \hat{\mathbf{Z}})$ sur $\mathbf{Q}^\star \backslash \mathrm{GL}(2, \mathbf{A}_f)$ est bien définie. Toutefois le sous-groupe de $\mathrm{GL}(2, \hat{\mathbf{Z}})$ qui stabilise $\mathrm{Isog}_{N,\zeta_N}(E)$ est celui défini par $\mathbf{dét}(\sigma) \equiv 1 \pmod{(N)}$, autrement dit $\mathrm{SL}(2, \hat{\mathbf{Z}}) \cdot \mathrm{GL}(2)[N\hat{\mathbf{Z}}]$. C'est un sous-groupe d'indice fini $\#\mathbf{Z}/(N)^\star$. Il est donc strict dès que $N \geq 3$. C'est sur ce sous-groupe que l'action sur $\mathrm{Isog}_{N,\zeta_N}(E)$ est bien définie.

Décrivons à présent l'action galoisienne. Posons $\boldsymbol{\mathcal{G}al}_L := \boldsymbol{\mathcal{G}al}(\mathbf{C}/L)$, pour tout corps $L \subseteq k$. Soient L, (E, β) et (E_L, β_L) comme dans l'énoncé. Soit aussi $\varphi : F \to E$ une isogénie. Alors φ induit l'isomorphisme $(\varphi, \hat{V}(\varphi))$ de $\mathcal{E}\ell\ell(\mathbf{C})'$ entre $(F, \hat{T}(F))$ et $(E, \hat{V}(\varphi)(\hat{T}(F)))$. Soit enfin $\sigma \in \boldsymbol{\mathcal{G}al}_L$. Décrivons E_L par une équation de Weierstraß à coefficients dans L. C'est une équation invariante sous σ. Par conséquent on pourra identifier les courbes complexes E et E^σ, car elles sont décrites par la même équation. Notons $\varphi^\sigma : F^\sigma \to E^\sigma = E$ l'isogénie tordue de φ. Alors $(F^\sigma, \hat{T}(F^\sigma))$ est isomorphe dans $\mathcal{E}\ell\ell(\mathbf{C})'$ à $(E, \hat{V}(\varphi^\sigma)(\hat{T}(F^\sigma)))$. Le carré suivant est commutatif

$$\begin{array}{ccc} F & \xrightarrow{\sigma_\star} & F^\sigma \\ \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \varphi^\sigma} \\ E & \xrightarrow{\sigma_\star} & E^\sigma \end{array}$$

si bien que $\hat{V}(\varphi^\sigma)(\hat{T}(F^\sigma)) = \rho(\sigma) \cdot \hat{V}(\varphi)(\hat{T}(F))$.

Considérons maintenant $\gamma : (\mathbf{Z}/(N))^2 \to F[N]$ une structure complète de niveau N et de racine associée ζ_N sur F. Alors $\gamma^\sigma = [\sigma_\star : F[N] \to F^\sigma[N]] \circ \gamma$ est la structure correspondante sur F. Cette dernière a également pour racine associée ζ_N, car par hypothèse σ fixe $\mathbf{Q}(\zeta_N)$.

En outre on a l'identité des deux isomorphismes: $\sigma_\star \circ \hat{T}(\varphi) \circ \gamma$ et $\hat{T}(\varphi^\sigma) \circ \sigma_\star \circ \gamma$ de $(\mathbf{Z}/(N))^2$ vers $\hat{V}(\varphi^\sigma)(\hat{T}(F^\sigma)) \otimes \mathbf{Z}/(N)$. En effet, le diagramme suivant commute:

$$\begin{array}{ccccc} (\mathbf{Z}/(N))^2 & \xrightarrow{\gamma} & F[N] & \xrightarrow{\sigma_\star} & F[N]^\sigma \\ & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \varphi^\sigma} \\ & & E[N] & \xrightarrow{\sigma_\star} & E[N]^\sigma \end{array}$$

Ainsi le réseau $\hat{V}(\varphi^\sigma)(\hat{T}(F^\sigma))$ de $\hat{V}(E)$ associé par φ^σ à la courbe F^σ et la classe d'isomorphisme relevant $(\mathbf{Z}/(N))^2 \xrightarrow{\sim} \hat{V}(\varphi^\sigma)(\hat{T}(F^\sigma)) \otimes \mathbf{Z}/(N)$ associée à $\sigma_\star \circ \gamma$ s'obtiennent à partir des éléments associés à F et γ par composition par $\sigma_\star : \hat{V}(E) \to \hat{V}(E)$.

Cela conclut la démonstration de la proposition 3.3, à ceci près qu'il faut établir que l'action $\boldsymbol{\mathcal{G}al}_L \to \mathrm{Aut}(\hat{T}(E))$ a un conoyau fini. C'est le propre du théorème suivant

Théorème 3.4 (de l'image ouverte de Serre, [19] et [20])**.** *Soit E une courbe elliptique (géométriquement) sans multiplication complexe définie sur un corps de nombres L. Alors l'action de $\boldsymbol{\mathcal{G}al}_L$ sur son module Tate $\hat{V}(E)$ se factorise par l'inclusion d'un sous-groupe d'indice fini de* $\mathrm{Aut}_{\hat{\mathbf{Z}}}(\hat{T}(E))$.

dans le cas où $j(E)$ est algébrique sur $\mathbf{Q}$. Dans le cas où $j(E)$ est transcendant, on utilise a un résultat analogue.

Proposition 3.5 (Corollaire[8] de [22], Théorème 6.6)**.** *Soit E une courbe elliptique complexe d'invariant j transcendant sur $\mathbf{Q}$. Alors pour tout entier $N \in \mathbf{N}_{>0}$, et tout automorphisme φ du groupe abélien $E[N]$, il existe un élément σ de $\boldsymbol{\mathcal{G}al}(\mathbf{C}/\mathbf{Q}(j(E))$ qui agit par φ sur $E[N]$.*

Démonstration. En effet $j(E)$ étant transcendant, il est *générique*, au sens du lemme 6.5, pour la fonction j sur $\mathfrak{H}$ et le corps dénombrable $k = \mathbf{Q}$. En outre (Théorème 6.6), les fonctions f_a, pour a dans $N^{-1}\mathbf{Z}^2 \setminus \mathbf{Z}^2$ sont algébriques sur $\mathbf{Q}(j)$. Dans la démonstration du lemme 6.5, il suffit de prendre pour f_1 la fonction j. Le sous-ensemble F_P de $\mathfrak{H}$ est alors le lieu où la fonction j prend des valeurs algébriques sur $\mathbf{Q}$. La démonstration conclut que tout z_0 tel que $j(z_0)$ est transcendant est générique au sens du lemme 6.5, à la fois pour la fonction j et les fonctions f_a, pour a dans $N^{-1}\mathbf{Z}^2 \setminus \mathbf{Z}^2$. On peut donc appliquer le théorème 6.6, et la remarque 6.7. □

Achevons à présent cette section en explicitant le plongement de l'ensemble

$$\mathbf{Q}^\star \backslash \mathrm{GL}(2, \mathbf{Q}) \mathrm{GL}(2)[N\hat{\mathbf{Z}}] / \mathrm{GL}(2)[N\hat{\mathbf{Z}}]$$

[8] La démonstration qui suit ne fait qu'expliciter les conditions d'utilisation du théorème 6.6 ([22]), et plus particulièrement l'affirmation «Actually we need this lemma only in the special case d=1 [...]» (p. 137).

dans $Y(N)(\mathbf{C})$ obtenu par identification avec $\mathrm{Isog}_{N,\zeta_N}(E)$. Plus précisément

Proposition 3.6. *On se place dans la situation de la proposition 3.3. Alors on a un carré commutatif*

$$\begin{array}{ccc} \mathbf{Q}^\star\backslash \mathrm{GL}(2,\mathbf{Q})\mathrm{GL}(2)[N\hat{\mathbf{Z}}]/\mathrm{GL}(2)[N\hat{\mathbf{Z}}] & \longrightarrow & \mathrm{Isog}_{N,\zeta_N}(E) \\ \downarrow & & \downarrow \\ \Gamma(N)\backslash(\mathrm{GL}(2,\mathbf{R})/\mathbf{R}^\star) & \longrightarrow & Y(N)(\mathbf{C}) \end{array}$$

où

- *la flèche supérieure est l'identification obtenue dans 3.1,*
- *la flèche de droite est l'inclusion naturelle,*
- *celle de gauche envoie $\mathbf{Q}^\star q\mathrm{GL}(2)[N\hat{\mathbf{Z}}]$ sur $\Gamma(N)(q^{-1}\mathbf{R}^\star)$, pour tout $q \in \mathrm{GL}(2,\mathbf{Q})$,*
- *et la flèche inférieure est donnée par $\Gamma(N)g\mathbf{R}^\star \mapsto g\cdot\tau$, où τ est un élément de $\mathfrak{H}$ relevant le point de $Y(N)(\mathbf{C})$ représentant la classe d'isomorphisme de (E,β).*

Démonstration. Il y a deux flèches à comparer: la composée de la flèche supérieure par la flèche de gauche d'une part, et la composée des deux autres flèches du carré d'autre part. Le groupe $\mathrm{GL}(2,\mathbf{Q})$ agit à gauche de façon transitive sur le double quotient $\mathbf{Q}^\star\backslash\mathrm{GL}(2,\mathbf{Q})\mathrm{GL}(2)[N\hat{\mathbf{Z}}]/\mathrm{GL}(2)[N\hat{\mathbf{Z}}]$. Il suffira donc de vérifier que les deux flèches à comparer prennent une valeur identique en au moins un même point, et qu'elles sont compatibles à l'action de $\mathrm{GL}(2,\mathbf{Q})$.

Considérons la double classe de la matrice identité. Elle correspond, dans $\mathrm{Isog}_{N,\zeta_N}$ et $Y(N)(\mathbf{C})$, à la classe de la courbe E elle-même munie de la structure induite par la base de $\hat{T}(E)$ que l'on s'est fixé.

Afin de prouver la compatibilité à l'action de $\mathrm{GL}(2,\mathbf{Q})$, choisissons un élément τ dans $\mathfrak{H}$ dont l'image dans $Y(N)(\mathbf{C})$ représente la classe de (E,β), et fixons un isomorphisme $\mathbf{C}/(\mathbf{Z}+\tau\mathbf{Z}) \to E(\mathbf{C})$ compatible aux structures de niveau. Considérons le morphisme additif

$$\lambda : \mathbf{Q}^2 \to \mathbf{C}$$

qui envoie (a,b) sur $a+b\tau$. On retrouve la structure β sur E en considérant l'image de la base $((1/N,0),(0,1/N))$ de $\mathbf{Q}^2$ dans $\mathbf{C}/(\lambda(\mathbf{Z}^2))$. Soit $g \in \mathrm{GL}(2,\mathbf{Q})$, et considérons le morphisme composé

$$\lambda \circ g : \mathbf{Q}^2 \to \mathbf{Q}^2 \to \mathbf{C}.$$

L'image du point $g\cdot\tau$ de $\mathfrak{H}$ dans $Y(N)(\mathbf{C})$ est représenté par la courbe $\mathbf{C}/(\lambda\circ g(\mathbf{Z}^2))$ munie de la base induite par $(\lambda\circ g(1/N,0), \lambda\circ g(0,1/N))$. On retrouve

ainsi, à isomorphisme près, toutes les structures de niveau N et de racine ζ_N sur des courbes elliptiques complexes isogènes à E.

Au niveau des modules de Tate, $\mathbf{C}/(\lambda(\mathbf{Z}^2))$ munie de sa structure de niveau N est représentée par l'isomorphisme $\lambda\otimes_{\mathbf{Q}}\mathbf{A}_f : {\mathbf{A}_f}^2 \to \lambda(\mathbf{Z}^2)\otimes_{\mathbf{Z}}{\mathbf{A}_f}^2$, et $\mathbf{C}/(\lambda\circ g(\mathbf{Z}^2))$ par l'isomorphisme composé à droite du précédent par l'isomorphisme ${\mathbf{A}_f}^2 \to {\mathbf{A}_f}^2$ de matrice g. Donc, pour $g \in \mathrm{GL}(2,\mathbf{Q})$, la classe d'isomorphisme de courbe elliptique avec structure de niveau N représentée par $g\tau$ est obtenu dans $\mathrm{Isom}({\mathbf{A}_f}^2, \mathbf{A}_f\otimes_{\mathbf{Z}}(\mathbf{Z}+\tau\mathbf{Z}))$ par l'action à gauche, par composition à droite, de g sur l'isomorphisme ${\mathbf{A}_f}^2 \to \mathbf{A}_f\otimes_{\mathbf{Z}}(\mathbf{Z}+\tau\mathbf{Z})$ donné par la base $(1,\tau)$. □

4 Autour des réseaux arithmétiques maximaux

L'objet de cette section est de démontrer le résultat de finitude sur les invariants j annoncé dans l'introduction (Prop. 4.10), mais également d'établir, ce faisant, divers énoncés de finitude, notamment la proposition 4.6 dont il sera fait usage par la suite.

Nous nous baserons sur les deux théorèmes suivants. Rappelons qu'un groupe algébrique semi-simple G sur $\mathbf{Q}$ est dit *de type non compact* s'il n'a aucun quasi-facteur (connexe) H tel que $H(\mathbf{R})$ soit compact. Nous n'aurons à utiliser dans les sections suivantes que le cas où $G = \mathrm{PGL}(2)$ ou $\mathrm{SL}(2)$.

Théorème 4.1 (A. Borel, [2])**.** *Le nombre de classes d'un groupe algébrique linéaire sur* $\mathbf{Q}$ *est fini.*

Autrement dit, pour tout sous-groupe ouvert K *de* $G(\mathbf{A}_f)$*,* $K\backslash G(\mathbf{A}_f)/G(\mathbf{Q})$ *est fini. Cela signifie aussi que* $G(\mathbf{A}_f)/\overline{G(\mathbf{Q})}$ *est compact.*

et

Théorème 4.2 (A. Borel, [3])**.** *Soit* G *un groupe algébrique linéaire semi-simple de type non compact sur* $\mathbf{Q}$*.*

Alors tout sous-groupe arithmétique de $G(\mathbf{C})$ *est contenu dans un nombre fini et non nul de sous-groupes arithmétiques maximaux distincts.*

Ces deux résultats sont dus, dans leur forme générale, à Armand Borel. Le second découle du *théorème de densité* de A. Borel, comme le rappelle la note [1]. Une autre référence se trouve dans [18], Théorème 4.10. Le premier est démontré dans [2], mais se trouve aussi dans [18], Théorèmes 5.1 et 8.1.

Sachant que tout groupe arithmétique Γ est de type fini ([5],V.20 ou [16], Théorème 3.1), on tire de 4.2 la conséquence suivante

Corollaire 4.3. *Soit* G *un groupe algébrique linéaire semi-simple de type non compact sur* $\mathbf{Q}$*.*

Alors tout sous-groupe arithmétique Γ *de* $G(\mathbf{C})$ *est contenu dans un nombre fini de sous-groupes arithmétiques.*

En effet soient $\Gamma_1, \ldots, \Gamma_k$ les sous-groupes arithmétiques maximaux de $G(\mathbf{C})$ contenant Γ, qui sont en nombre fini d'après 4.2. Soit B l'indice maximal de Γ dans l'un des Γ_i. Comme les Γ_i sont de type fini, ils ne contiennent chacun qu'un nombre fini de sous-groupes d'indice au plus B. Or tout sous-groupe arithmétique contenant Γ est contenu dans l'un des Γ_i, et ce avec un indice au plus B, ce qui démontre le corollaire.

Nous en déduisons la première propriété de finitude suivante

Proposition 4.4. *Soit G un groupe algébrique linéaire sur $\mathbf{Q}$, semi-simple de type non compact. Soit $(\Gamma_n)_{n\in\mathbf{N}}$ une suite, supposée sans sous-suite constante, de sous-groupes arithmétiques de $G(\mathbf{Q})$ deux à deux conjugués. Soit Γ un sous-groupe arithmétique quelconque de $G(\mathbf{Q})$.*

Alors $[\Gamma : \Gamma \cap \Gamma_n]$ et $[\Gamma_n : \Gamma \cap \Gamma_n]$ tendent vers $+\infty$.

Démonstration. Supposons par l'absurde qu'il existe un entier B tel que l'inégalité $[\Gamma : \Gamma \cap \Gamma_n] \leq B$ soit vérifiée pour une infinité d'indices n. Comme Γ est de type fini, il n'a qu'un nombre fini de sous-groupes de Γ d'indice au plus B. Donc la famille des $\Gamma \cap \Gamma_n$, lorsque n parcourt ces indices, ne comprend qu'un nombre fini de membres. D'après le corollaire, appliqué à chacun de ces éléments, il n'y a qu'un nombre fini de sous-groupes arithmétiques de $G(\mathbf{C})$ contenant l'un de ces $\Gamma \cap \Gamma_n$. Or la suite des Γ_n est supposée sans sous-suite constante; c'est la contradiction recherchée. On a ainsi montré que la suite $[\Gamma : \Gamma \cap \Gamma_n]$ tend vers l'infini.

Choisissons, pour chaque entier naturel n, un élément g_n de $G(\mathbf{Q})$ tel que l'on ait $\Gamma_n = g_n \Gamma_0 {g_n}^{-1}$. Alors la conjugaison par ${g_n}^{-1}$ induit une bijection

$$\Gamma_n/\Gamma \cap \Gamma_n \xrightarrow{\sim} \Gamma_0/({g_n}^{-1}\Gamma g_n) \cap \Gamma_0.$$

On en déduit que $[\Gamma_n : \Gamma \cap \Gamma_n] = [\Gamma_0 : ({g_n}^{-1}\Gamma g_n) \cap \Gamma_0]$.

J'affirme alors que la suite des ${g_n}^{-1}\Gamma g_n$ n'admet pas de sous-suite constante. En effet, la suite d'entiers $[\Gamma : \Gamma \cap \Gamma_n] = [({g_n}^{-1}\Gamma g_n) : ({g_n}^{-1}\Gamma g_n) \cap \Gamma_0]$ n'admet pas de sous-suite constante; elle tend, on l'a vu, vers l'infini.

Quitte à échanger les rôles de Γ et Γ_0 et à étudier la suite des ${g_n}^{-1}\Gamma_0 g_n$, le raisonnement par l'absurde ci-dessus s'applique et on conclut que $[\Gamma_n : \Gamma \cap \Gamma_n] = [\Gamma_0 : ({g_n}^{-1}\Gamma g_n) \cap \Gamma_0]$ tend également vers ∞. □

Il nous faut maintenant établir l'analogue adélique de l'énoncé précédent. On renvoie à la section précédente pour les notations utilisées, concernant les adèles. Il nous faudra, pour ce, faire usage de la propriété de finitude du nombre de classes. Dans les énoncés suivants on identifiera le groupe $G(\mathbf{Q})$ avec son image dans $G(\mathbf{A}_f)$ induite par le morphisme d'anneaux $\mathbf{Q} \to \mathbf{A}_f$.

Proposition 4.5. *Soit G un groupe algébrique linéaire sur $\mathbf{Q}$, semi-simple de type non compact. Soit $(K_n)_{n\in\mathbf{N}}$ une suite, supposée sans sous-suite constante,*

de sous-groupes compacts, ouverts, et deux à deux conjugués, de $G(\mathbf{A}_f)$. *Soit* K *un sous-groupe compact ouvert de* $G(\mathbf{A}_f)$. *Notons* $\Gamma = G(\mathbf{Q}) \cap K$ *et* $\Gamma_n = G(\mathbf{Q}) \cap K_n$.

Alors les suites d'entiers $[\Gamma : \Gamma \cap \Gamma_n]$ *et* $[\Gamma_n : \Gamma \cap \Gamma_n]$, *ainsi que les suites* $[K : K \cap K_n]$ *et* $[K_n : K \cap K_n]$, *tendent vers* $+\infty$.

Démonstration. Soient K et K' deux sous groupes compacts et ouverts de $G(\mathbf{A}_f)$. Alors $K/K \cap K'$ est fini. Soient $\Gamma = K \cap G(\mathbf{Q})$ et $\Gamma' = K' \cap G(\mathbf{Q})$ les groupes arithmétiques associés. Alors l'application canonique

$$\Gamma/\Gamma \cap \Gamma' \longrightarrow K/K \cap K'$$

est injective. On a donc une minoration $[K : K \cap K'] \geq [\Gamma : \Gamma \cap \Gamma']$. Par conséquent, il nous suffira de ne démontrer la conclusion uniquement qu'en ce qui concerne les groupes Γ et Γ_n.

Par la propriété 4.1 de finitude du nombre de classes appliquée au sous-groupe ouvert K_0 de $G(\mathbf{A}_f)$, il existe un sous-ensemble fini F de $G(\mathbf{A}_f)$ tel que $G(\mathbf{A}_f) = G(\mathbf{Q}) \cdot F \cdot K_0$. En particulier, pour chaque $n \in \mathbf{N}$, on peut trouver une écriture du sous-groupe K_n, conjugué à K_0 dans $G(\mathbf{A}_f)$, sous la forme

$$K_n = q_n f_n K_0 {f_n}^{-1} {q_n}^{-1}, \text{ où } f_n \in F_{K_0} \text{ et } q_n \in G(\mathbf{Q}).$$

Notons $\Gamma_f = f K_0 f^{-1} \cap G(\mathbf{Q})$ pour $f \in F$, et $\Gamma_{f,n} = q_n \Gamma_f {q_n}^{-1}$ pour $(f, n) \in F \times \mathbf{N}$. On a ainsi $\Gamma_{f_n,n} = K_n \cap G(\mathbf{Q})$ pour tout $n \in \mathbf{N}$. Enfin Γ désignera $K \cap G(\mathbf{Q})$.

On va montrer que pour tout f dans F, la suite des $\Gamma_{f,n}$ n'admet pas de sous suite constante. Notons $\mathrm{N}(\Gamma_f)$ le normalisateur de Γ_f dans $G(\mathbf{Q})$. C'est sous-groupe arithmétique de $G(\mathbf{Q})$ contenant Γ_f: L'indice $[\mathrm{N}(\Gamma_f) : \Gamma_f]$ est fini (cf. [14], (5.43)).

Cela revient à montrer que la suite $(q_n \cdot \mathrm{N}(\Gamma_f))_{n \in \mathbf{N}}$ des classes à droite modulo $\mathrm{N}(\Gamma_f)$ n'a pas de sous-suite constante. Il suffit, $[\mathrm{N}(\Gamma_f) : \Gamma_f]$ étant fini, que ce soit le cas pour la suite $(q_n \cdot \Gamma_f)_{n \in \mathbf{N}}$, ou même, F étant fini, pour la suite $\left(q_n \cdot (\bigcap_{f \in F} \Gamma_f)\right)_{n \in \mathbf{N}}$.

Supposons, par l'absurde, que la classe $q_n \cdot \bigcap_{f \in F} \Gamma_f$ soit la même pour une infinité d'indices n. Quitte à extraire, F étant fini, on peut supposer qu'en outre, pour ces indices, f_n ne prend qu'une seule valeur, disons g. Dès lors, $K_n = q_n (g K_0 g^{-1}) {q_n}^{-1}$ ne prend qu'une seule valeur lorsque n parcourt ces mêmes indices, car d'une part Γ_g est contenu dans $g K_0 g^{-1}$, et d'autre part $q_n \Gamma_g$ est supposé ne pas dépendre de n. Or K_n étant supposé sans sous-suite constante, c'est absurde.

On en déduit que pour tout $n \in \mathbf{N}$ il n'y a qu'un nombre fini d'indices n' tels que $\Gamma_{f,n} = \Gamma_{f,n'}$.

Ainsi la suite des $\Gamma_{f,n}$ n'admet pas de sous-suite constante.

On peut alors appliquer la proposition précédente, et en déduire que pour f fixé $[\Gamma : \Gamma \cap \Gamma_{f,n}]$ tend vers $+\infty$. On conclut alors, par finitude de F, que les suites $[\Gamma_{f,n} : \Gamma \cap \Gamma_{f,n}]$ et $[\Gamma : \Gamma \cap \Gamma_{f,n}]$ tendent vers $+\infty$. □

La prochaine étape consiste à obtenir le résultat analogue pour les *orbites* dans $G(\mathbf{A}_f)/K'$ d'un sous-groupe compact ouvert K de $G(\mathbf{A}_f)$ plutôt qu'à l'image des conjugués de K. Ici K' désigne un deuxième sous-groupe compact ouvert de $G(\mathbf{A}_f)$.

Proposition 4.6. *Soit G un groupe algébrique linéaire sur $\mathbf{Q}$, semi-simple de type non compact. Soient K et K' deux sous-groupes compacts ouverts de $G(\mathbf{A}_f)$. Soit $(g_n)_{n\in\mathbf{N}}$ une suite dans $G(\mathbf{A}_f)$ telle que les K-orbites Kg_nK'/K' soient deux à deux distinctes dans $G(\mathbf{A}_f)/K'$.*

Alors la suite d'entiers $\#Kg_nK'/K'$ tend vers $+\infty$. En outre, en notant $\Gamma = G(\mathbf{Q}) \cap K$, $\#\Gamma g_nK'/K'$ tend également vers $+\infty$.

Démonstration. Étant donné $g \in G(\mathbf{A}_f)$, nous avons des bijections

$$\begin{array}{rcccl} KgK'/K' & \xrightarrow{\sim} & g^{-1}KgK' & / & K' \\ & \simeq & g^{-1}Kg & / & (K' \cap g^{-1}Kg) \\ & \xrightarrow{\sim} & K & / & (gK'g^{-1} \cap K), \end{array}$$

d'où l'égalité $\#KgK'/K' = [K : gK'g^{-1} \cap K]$.

Montrons maintenant que la correspondance suivante

$$\left\{(KgK', g^{-1}Kg) | g \in G(\mathbf{A}_f)\right\}$$

entre doubles classes de K et K' et conjugués de K est une correspondance *finie*. Cette correspondance est induite par les flèches

$$\begin{array}{ccccc} K\backslash G(\mathbf{A}_f)/K' & \longleftarrow & K\backslash G(\mathbf{A}_f) & \longrightarrow & \mathrm{N}(K)\backslash G(\mathbf{A}_f), \\ KgK' & \longmapsto & Kg & \longmapsto & g^{-1}Kg. \end{array}$$

où $\mathrm{N}(K)$ désigne le normalisateur de K. Il suffit donc de montrer que chacune de ces deux flèches est à fibres finies.

Pour la flèche de gauche, KgK' étant compact, son image dans $K\backslash G(\mathbf{A}_f)$ est finie, K étant ouvert.

Pour la flèche de droite il faut montrer que $\mathrm{N}(K)/K$ est fini. Il suffit de montrer que $\mathrm{N}(K)$ est compact, K étant ouvert.

Proposition 4.7. *Soit G un groupe algébrique semi-simple sur $\mathbf{Q}$. Soit K un sous-groupe ouvert et compact de $G(\mathbf{A}_f)$. Alors le normalisateur $\mathrm{N}(K)$ de K dans $G(\mathbf{A}_f)$ est compact.*

Démonstration. La démonstration commence avec le fait bien connu suivant, où, pour un sous-groupe algébrique de $GL(N)$ défini sur $\mathbf{Q}$ on note $G(\mathbf{Z}_p)$ le sous-groupe des points de $G(\mathbf{Q}_p)$ qui appartiennent à $\mathrm{GL}(N, \mathbf{Z}_p)$ et $G(\hat{\mathbf{Z}})$ le produit des $G(\mathbf{Z}_p)$ pour p premier.

Lemme 4.8. *Soit G un sous-groupe algébrique de $\mathrm{GL}(N)$ défini sur $\mathbf{Q}$, et K un sous-groupe compact ouvert de $G(\mathbf{A}_f)$. Alors il existe un ensemble fini F de nombres premiers, arbitrairement grand, et un sous-groupe compact et ouvert K_F de $G(\prod_{p\in F}\mathbf{Q}_p)$ tels que*

$$K = K_F \times \prod_{p\notin F} G(\mathbf{Z}_p).$$

En effet K et $G(\hat{\mathbf{Z}})$ étant compacts et ouverts, ce sont des sous-groupes commensurables de $G(\mathbf{A}_f)$. Il existe donc un sous-ensemble fini E de $G(\mathbf{A}_f)$ tel que $K \subseteq E \cdot G(\hat{\mathbf{Z}})$ et $G(\hat{\mathbf{Z}}) \subseteq E \cdot K$. Soit F un ensemble fini de nombres premiers contenant ceux apparaissant aux dénominateurs des éléments de E. C'est un ensemble fini arbitrairement grand et, par construction, il vérifie

$$\prod_{p\notin F}\{1\} \times \prod_{p\notin F} G(\mathbf{Z}_p) \subseteq K \subseteq \prod_{p\in F} G(\mathbf{Q}_p) \times \prod_{p\notin F} G(\mathbf{Z}_p).$$

Il en découle le résultat cherché.

Avant de terminer la démonstration de 4.7, nous établissons une conséquence de [18], Prop. 3.16.

Proposition 4.9. *Soit G un groupe algébrique semi-simple sur $\mathbf{Q}$, soit F un ensemble fini de nombres premiers, et soit K un sous-groupe ouvert et compact de $\prod_{p\in F} G(\mathbf{Q}_p)$. Alors le normalisateur $\mathrm{N}(K)$ de K dans $\prod_{p\in F} G(\mathbf{Q}_p)$ est compact.*

En effet introduisons, pour tout p dans F, le sous-groupe $K_p := K \cap G(\mathbf{Q}_p)$ de K. C'est un sous-groupe compact et ouvert de $G(\mathbf{Q}_p)$. Donc, d'après [18], Prop. 3.16, son normalisateur $\mathrm{N}_{G(\mathbf{Q}_p)}(K_p)$ dans $G(\mathbf{Q}_p)$ est compact. Soit maintenant un élément $g = (g_p)_{p\in F}$ de $\prod_{p\in F} G(\mathbf{Q}_p)$ normalisant K. Comme $G(\mathbf{Q}_p)$ est un sous-groupe normal de $\prod_{p\in F} G(\mathbf{Q}_p)$, g_p appartient à $\mathrm{N}_{G(\mathbf{Q}_p)}(K_p)$, pour tout élément p de F. Il suit que $\mathrm{N}(K)$ s'identifie à un sous-groupe de $\prod_{p\in F} \mathrm{N}_{G(\mathbf{Q}_p)}(K_p)$, qui est compact. Comme $\mathrm{N}(K)$ est un sous-groupe fermé, on en déduit qu'il est compact.

Démontrons à présent la proposition 4.7. En effet soit G un groupe algébrique semi-simple, et considérons une représentation fidèle de G sur $\mathbf{Q}$, de sorte que G peut-être vu comme sous-groupe fermé de $GL(N)$.

D'après [26], Prop. 3.9.1, pour tout nombre premier p, hormis un ensemble fini E d'entre eux, $G(\mathbf{Z}_p)$ est un sous-groupe (compact) *hyperspécial* de $G(\mathbf{Q}_p)$. En particulier, c'est un sous-groupe compact maximal ([26], 3.8.2) de $G(\mathbf{Q}_p)$.

Pour un tel p, considérons le normalisateur de $G(\mathbf{Z}_p)$ dans $G(\mathbf{Q}_p)$. C'est un groupe compact, d'après [18], Prop. 3.16, et ce groupe contient $G(\mathbf{Z}_p)$. Le groupe $G(\mathbf{Z}_p)$ étant compact maximal, il est donc son propre normalisateur.

Soit enfin K un sous-groupe compact et ouvert de $G(\mathbf{A}_f)$. D'après le lemme 4.8, il existe un ensemble fini F de nombres premiers tels que K peut se mettre sous la forme $K_F \times \prod_{p\notin F} G(\mathbf{Z}_p)$. On peut même supposer que l'ensemble fini E ci-dessus est contenu dans F. Le normalisateur de K dans $G(\mathbf{A}_f)$ s'écrit alors

$$\mathrm{N}(K) = \mathrm{N}_{G(\prod_{p\in F}\mathbf{Q}_p)}(K_F) \times \prod_{p\notin F} G(\mathbf{Z}_p).$$

D'après la proposition 4.9, $\mathrm{N}_{G(\prod_{p\in F}\mathbf{Q}_p)}(K_F)$ est un sous-groupe compact. On peut alors conclure que $N(K)$ est un sous-groupe compact de $G(\mathbf{A}_f)$. □

On peut à présent terminer la démonstration de la proposition 4.6. Dans l'égalité $\#KgK'/K' = [K : gK'g^{-1} \cap K]$, il n'y a, d'après 4.7, qu'un nombre fini de doubles classes KgK' qui correspondent à un conjugué donné gKg^{-1} de K. On peut alors conclure à la première partie de l'énoncé en appliquant la proposition 4.5.

Quant à la seconde partie de la conclusion, on écrit, par finitude du nombre de classes, $g_n = q_n \cdot f_n \cdot k_n$, où $q_n \in G(\mathbf{Q})$, $k_n \in K'$ et $f_n \in F$ et où F est un sous-ensemble fini de $G(\mathbf{A}_f)$. Quitte à extraire une sous-suite on peut supposer que f_n ne dépend pas de n. Quitte à remplacer K' par $f_0 K' {f_0}^{-1}$, qui lui est commensurable, on peut même supposer que f_n est l'élément neutre ou, ce qui revient au même que $g_n \in G(\mathbf{Q})$. Dès lors $\Gamma g_n K'/K'$ est canoniquement isomorphe à $\Gamma g_n \Gamma'/\Gamma'$, où $\Gamma' := K' \cap G(\mathbf{Q})$. Or la correspondance précédente induit une sous-correspondance

$$\begin{array}{ccccc} \Gamma\backslash G(\mathbf{Q})/\Gamma' & \longleftarrow & \Gamma\backslash G(\mathbf{Q}) & \longrightarrow & \mathrm{N}(\Gamma)\backslash G(\mathbf{Q}), \\ \Gamma g \Gamma' & \longleftarrow\!\shortmid & \Gamma g & \shortmid\!\longrightarrow & g^{-1}\Gamma g \end{array}$$

elle aussi finie. Il suffit, pour conclure, d'appliquer la proposition 4.5. □

Nous appliquons maintenant ce résultat au groupe PGL(2) et en déduisons, par le biais du théorème de l'image ouverte dans le cas algébrique, et la proposition 3.5 sinon, une propriété de finitude sur les j-invariants.

Proposition 4.10. *Soit L un sous-corps de $\mathbf{C}$ de type fini sur $\mathbf{Q}$ et soit E une courbe elliptique complexe sans multiplication complexe définissable sur une extension finie de L. Soit $(E_n)_{n\in\mathbf{N}}$ une suite de courbes elliptiques toutes isogènes à E mais deux à deux non isomorphes. Alors* $\deg_L(j(E_n)) \to +\infty$.

Démonstration. Soit E_K un modèle de sur une extension finie K de L. Alors on a l'encadrement $1 \leq \deg_L(j(E_n))/\deg_K(j(E_n)) \leq [K : L]$. Il suffit par

conséquent de considérer la suite des entiers $\deg_K(j(E_n))$. Or $\deg_K(j(E_n))$ est le cardinal de l'orbite de $j(E_n)$ sous l'action de $\boldsymbol{\mathcal{G}al}(\mathbf{C}/K)$.

La $\boldsymbol{\mathcal{G}al}(\mathbf{C}/K)$-orbite de chacun des $j(E_n)$ étant finie, on peut bien sûr remplacer l'hypothèse que les E_n sont non isomorphes, autrement dit que les $j(E_n)$ sont distincts, par l'hypothèse que leurs $\boldsymbol{\mathcal{G}al}(\mathbf{C}/K)$-orbites sont deux à deux distinctes.

Nous avons vu que l'action de $\boldsymbol{\mathcal{G}al}(\mathbf{C}/K)$ sur l'ensemble des j-invariants provenant de courbe elliptiques isogènes à E est isomorphe à l'action d'un sous-groupe ouvert de $\mathrm{PGL}(2,\hat{\mathbf{Z}})$ sur $\mathrm{PGL}(2,\mathbf{Q})/\mathrm{PGL}(2,\mathbf{Z})$ (Proposition 3.3.) .

Or d'après la proposition 4.6, cette action n'admet, pour tout entier N, qu'un nombre fini d'orbites de cardinal au plus N. □

5 Équidistribution des points de Hecke

Le résultat principal de cette section est la proposition 5.2, qui n'est qu'une variante adélique déduite du résultat d'équidistribution des *points de Hecke*. Nous entendrons par ce terme les classes provenant d'un réseau d'un groupe de Lie, pour l'action d'un second réseau commensurable au premier. Plus précisément nous nous baserons sur l'énoncé suivant

Théorème 5.1 (Équidistribution des points de Hecke, cf. [9])**.** *Soit G un groupe algébrique linéaire $\mathbf{Q}$-simple connexe tel que $G(\mathbf{R})$ est non compact. Soient Γ et Γ' deux réseaux arithmétiques de $G(\mathbf{R})^+$. Notons μ l'unique probabilité $G(\mathbf{R})^+$ invariante sur $\Gamma'\backslash G(\mathbf{R})^+$. Considérons une suite $(g_n)_{n\in\mathbf{N}}$ telle que les Γ-orbites*

$$\Gamma'\backslash\Gamma' g_n\cdot\Gamma$$

sont deux à deux distinctes dans $\Gamma'\backslash G(\mathbf{R})^+$.

Alors pour toute fonction continue et bornée $f:\Gamma'\backslash G(\mathbf{R})^+\longrightarrow\mathbf{R}$,

$$\frac{\sum_{x\in\Gamma'\backslash\Gamma' g_n\cdot\Gamma} f(x)}{\#\Gamma'\backslash\Gamma' g_n\cdot\Gamma}\to\mu(f):=\int_{\Gamma'\backslash G(\mathbf{R})^+} f\,d\mu.$$

En d'autres termes, les orbites $\Gamma'\backslash\Gamma' g_n\cdot\Gamma$ *s'équidistribuent* dans $\Gamma'\backslash G(\mathbf{R})^+$ vers la probabilité homogène μ.

Dans cet énoncé la notation $G(\mathbf{R})^+$ désigne la composante neutre du groupe de Lie réel $G(\mathbf{R})$. C'est un groupe de Lie réel *connexe*.

Nous traitons ici le cas d'un groupe algébrique aussi général que possible. Nous nous référons à [9][9] où le résultat suivant se déduit directement de l'étude du théorème de Ratner issue de [15]. Pour nos applications dans le contexte

[9] À noter toutefois que, dans le cas arithmétique tout au moins, l'hypothèse supplémentaire de [9] sur les degrés est superflue, d'après la proposition 4.6.

adélique, il semble que l'énoncé contenu dans [4] suffise. Pour la démonstration du résultat 2.1, nous n'utiliserons que le cas du groupe SL(2), ou plutôt de PGL(2). Il se pourrait alors que le résultat de [4] soit connu de plus longue date pour ce groupe particulier.

Pour démontrer le résultat 2.1, nous utiliserons la variante adélique ci-dessous de cet énoncé. On prendra garde à différencier les copies suivantes de $\mathbf{Q}$: l'image $\iota_{\mathbf{R}}(\mathbf{Q})$ de $\iota_{\mathbf{R}} : \mathbf{Q} \to \mathbf{R}$, l'image $\iota_f(\mathbf{Q})$ de $\iota_f : \mathbf{Q} \to \mathbf{A}_f$ et l'image $\iota_{\mathbf{A}}(\mathbf{Q})$ de $\iota_{\mathbf{A}} : \mathbf{Q} \to \mathbf{A}$, plus simplement notée $\mathbf{Q}$. Le groupe $G(\mathbf{Q})^+ \leq G(\mathbf{A})$ désigne alors la préimage de $G(\mathbf{R})^+$, et ses images par $\iota_{\mathbf{R}}$ et ι_f seront respectivement notées $G(\iota_{\mathbf{R}}(\mathbf{Q}))^+$ et $G(\iota_f(\mathbf{Q}))^+$.

Remarquons que par finitude du nombre de classes, il existe pour tout sous-groupe compact et ouvert K' de $G(\mathbf{A}_f)$ un ensemble fini F, dépendant de K', tel que

$$G(\mathbf{A}) = G(\mathbf{Q}) \cdot F \cdot G(\mathbf{R})^+ K'.$$

Soit Γ' le réseau $\iota_{\mathbf{R}} \circ {\iota_f}^{-1}(K' \cap G(\iota_f(\mathbf{Q}))^+)$ de $G(\mathbf{R})^+$. Alors l'application naturelle

$$\Gamma' \backslash G(\mathbf{R})^+ \to G(\mathbf{Q}) \backslash G(\mathbf{Q}) \cdot G(\mathbf{R})^+ \cdot K'/K'$$

induit un isomorphisme de $G(\mathbf{R})^+$-espaces homogènes à droite. En particulier $G(\mathbf{Q}) \backslash G(\mathbf{Q}) \cdot G(\mathbf{R})^+ \cdot K'/K'$ est connexe.

Proposition 5.2. *Soit G un groupe algébrique linéaire $\mathbf{Q}$-simple connexe de type non compact. Soient K et K' deux sous-groupes compacts et ouverts de $G(\mathbf{A}_f)$. Considérons une suite $(g_n)_{n \in \mathbf{N}}$ dans $G(\iota_f(\mathbf{Q}))^+$ telle que les K-orbites*

$$K \cdot g_n \cdot K'/K'$$

soient deux à deux distinctes dans $G(\mathbf{A}_f)/K'$. On considérera les sous-ensembles $E_n = (K \cdot g_n) \cap \left(\overline{G(\iota_f(\mathbf{Q}))^+} \cdot K'\right)$ de $G(\mathbf{A}_f)/K'$.

On désigne par μ la probabilité $G(\mathbf{R})^+$-invariante sur le $G(\mathbf{R})^+$-espace homogène à droite connexe $\mathbf{X} := G(\mathbf{Q}) \backslash G(\mathbf{Q}) \cdot G(\mathbf{R})^+ \cdot K'/K'$.

Alors pour toute fonction continue et bornée $f : \mathbf{X} \to \mathbf{R}$,

$$\frac{\sum_{x \in G(\mathbf{Q}) \backslash G(\mathbf{Q}) \cdot E_n \cdot K'/K'} f(x)}{\#G(\mathbf{Q}) \backslash G(\mathbf{Q}) \cdot E_n \cdot K'/K'} \to \mu(f) := \int_{\mathbf{X}} f \, d\mu.$$

En d'autres termes, la suite des ensembles finis $E_n \cdot K'/K'$ s'équidistribue dans $G(\mathbf{Q}) \backslash G(\mathbf{Q}) \cdot G(\mathbf{R})^+ \cdot K'/K' \simeq \Gamma' \backslash G(\mathbf{R})^+$ pour μ.

Comme K' est ouvert et K est compact, $K \cdot g_n \cdot K'/K'$ est un sous-ensemble fini de l'espace discret $G(\mathbf{A}_f)/K'$. On peut donc remplacer l'hypothèse que les K-orbites $K \cdot g_n \cdot K'/K'$ soient deux à deux distinctes par l'hypothèse que $g_n \cdot K'$ tende vers l'infini dans $G(\mathbf{A}_f)/K'$. Comme K' est compact, cela revient au même de supposer que g_n tend vers l'infini dans $G(\mathbf{A}_f)$.

Cela étant, la proposition 4.6 permet déjà d'affirmer que la suite de cardinaux $\#K \cdot g_n \cdot K'/K'$ tend vers $+\infty$ si et seulement si g_n tend vers ∞ dans $G(\mathbf{A}_f)$. Or l'application $G(\mathbf{A}_f)/K' \to G(\mathbf{Q})\backslash G(\mathbf{A})/K'$ est injective. Par conséquent le cardinal de $G(\mathbf{Q})\backslash G(\mathbf{Q}) \cdot K \cdot g_n \cdot K'/K'$ égale celui de $K \cdot g_n \cdot K'/K'$. Sous les hypothèses de l'énoncé, ces cardinaux tendent donc vers $+\infty$.

La réduction de la proposition 5.2 au théorème 5.1 précédente consiste essentiellement en l'application du lemme suivant

Lemme 5.3. *Soient donnés l'action quelconque d'un groupe $\mathcal{G}$ sur un ensemble X, ainsi qu'un sous-groupe $\mathcal{H}$ de $\mathcal{G}$ et un sous-ensemble $\mathcal{H}$-stable Y de X. Soit également $f : Y \to Z$ une application vers un espace localement compact.*

On considère une suite $\mathcal{G} \cdot x_n$ d'orbites finies de $\mathcal{G}$ dans X rencontrant Y. Supposons que pour toute suite y_n de Y, telle que $y_n \in \mathcal{G} \cdot x_n \cap Y$ pour tout $n \in \mathbf{N}$, la suite de probabilités $f_\star \mu_{y_n}$ sur Z converge vers une unique probabilité μ, où μ_{y_n} désigne la probabilité $\mathcal{H}$-invariante de support $\mathcal{H} \cdot y_n$.

Alors en désignant par μ_n la probabilité équidistribuée de support $\mathcal{G} \cdot x_n \cap Y$, la suite $f_\star \mu_n$ converge également vers μ, lorsque $n \to \infty$.

Notons en passant qu'il sera ultérieurement fait usage du cas particulier suivant où $X = Y = Z$ et f est l'identité

Lemme 5.4. *Soient donnés l'action quelconque d'un groupe $\mathcal{G}$ sur un espace localement compact X, ainsi qu'un sous-groupe $\mathcal{H}$ de $\mathcal{G}$. Considérons une suite $(x_n)_{n\in\mathbf{N}}$ dans X telle que l'orbite $\mathcal{G} \cdot x_n$ est finie pour tout $n \in \mathbf{N}$.*

Supposons que pour toute suite $(y_n)_{n\in\mathbf{N}}$ telle que $y_n \in \mathcal{G} \cdot x_n$ pour tout $n \in \mathbf{N}$, μ_{y_n} converge vers μ, où μ_{y_n} désigne la probabilité $\mathcal{H}$-invariante supportée par $\mathcal{H} \cdot y_n$.

Alors si μ_n désigne la probabilité $\mathcal{G}$-invariante sur $\mathcal{G} \cdot x_n$, μ_n tend vers μ.

Démonstration. Soit φ une fonction continue et bornée sur Z. On veut montrer

$$\text{« } \mu_n(\varphi) = \frac{\sum_{x\in(\mathcal{G}\cdot x_n)\cap Y} \varphi \circ f(x)}{\#\left((\mathcal{G} \cdot x_n) \cap Y\right)} \text{ tend vers } \mu(f) \text{ lorsque } n \text{ tend vers } \infty \text{ »}$$

Or on peut réarranger la somme finie ainsi

$$\mu_n(\varphi) = \frac{\sum_{E\in\mathcal{H}\backslash(\mathcal{G}\cdot x_n)\cap Y}}{\#\left(\mathcal{H}\backslash(\mathcal{G} \cdot x_n) \cap Y\right)} \left(\frac{\sum_{x\in E} \varphi \circ f(x)}{\#E} \right).$$

Par hypothèse, l'ensemble de réels $\left\{\sum_{x\in E} \varphi \circ f(x)/\#E | E \in \mathcal{H}\backslash(\mathcal{G} \cdot x_n) \cap Y\right\}$ tend uniformément vers $\mu(\varphi)$ lorsque n tend vers ∞. On conclut donc que $\mu_n(\varphi)$, qui en est un barycentre, tend lui aussi vers $\mu(\varphi)$. □

Démontrons sans tarder la proposition 5.2.

Démonstration. Utilisons le lemme 5.3 pour $X = G(\mathbf{A}_f)/K'$, $\mathcal{G} = K$, $\mathcal{H} = K \cap G(\iota_f(\mathbf{Q}))^+$, $Y = \overline{G(\iota_f(\mathbf{Q}))^+}/K'$, $Z = G(\mathbf{Q})\backslash G(\mathbf{Q})G(\mathbf{R})^+K'/K'$ et une suite $K \cdot g_n \cdot K'/K'$ de $\mathcal{G}$-orbites telle que dans l'énoncé de la proposition. Nous en déduisons qu'il suffit d'établir la convergence en ne considérant que des $K \cap G(\iota_f(\mathbf{Q}))^+$-orbites contenues dans Y plutôt que des K-orbites.

Introduisons les sous-groupes Γ et Γ' de $G(\mathbf{Q})$ tels que $\iota_f(\Gamma) = K \cap G(\iota_f(\mathbf{Q}))^+$ et $\iota_f(\Gamma') = K' \cap G(\iota_f(\mathbf{Q}))^+$. Ainsi $\iota_{\mathbf{R}}(\Gamma)$ et $\iota_{\mathbf{R}}(\Gamma')$ forment des réseaux arithmétiques de $G(\mathbf{R})^+$.

Établissons la commutativité du diagramme ci-dessous

$$\begin{array}{ccc} G(\mathbf{Q})^+/\Gamma' & \longrightarrow & \Gamma'\backslash G(\mathbf{Q})^+ \\ \downarrow & & \downarrow \\ \overline{G(\iota_f(\mathbf{Q}))^+} \cdot K'/K' & & \iota_{\mathbf{R}}(\Gamma')\backslash G(\mathbf{R})^+ \\ & \searrow \quad \swarrow & \\ & G(\mathbf{Q})\backslash G(\mathbf{Q}) \cdot G(\mathbf{R})^+ \cdot K'/K' & \end{array}$$

où la flèche horizontale est la bijection: $q^{-1}\Gamma' \mapsto \Gamma' q$. Il suffit de remarquer que pour $q \in G(\mathbf{Q})$, les $G(\mathbf{Q})$-classes à gauche $G(\mathbf{Q}) \cdot G(\iota_{\mathbf{R}})(q)$ et $G(\mathbf{Q}) \cdot G(\iota_f)(q^{-1})$ sont identiques dans $G(\mathbf{Q})\backslash G(\mathbf{A})$.

Ainsi les orbites à gauche $\iota_f(\Gamma) \cdot g_n \cdot K'/K'$ de $\iota_f(\Gamma)$ dans $G(\iota_f(\mathbf{Q}))^+ \cdot K'/K'$ et les orbites à droite $\iota_{\mathbf{R}}(\Gamma')\backslash\iota_{\mathbf{R}}(\Gamma') \cdot G({\iota_{\mathbf{R}}} \circ {\iota_f}^{-1})(g_n) \cdot \iota_{\mathbf{R}}(\Gamma)$ de $\iota_{\mathbf{R}}(\Gamma)$ dans $\iota_{\mathbf{R}}(\Gamma')\backslash G(\mathbf{R})^+$ induisent le même ensemble dans $G(\mathbf{Q})\backslash G(\mathbf{Q}) \cdot G(\mathbf{R})^+ \cdot K'/K'$. On s'est donc ramené à établir l'équidistribution de $\iota_{\mathbf{R}}(\Gamma)$-orbites dans $\iota_{\mathbf{R}}(\Gamma')\backslash G(\mathbf{R})^+$.

Or les K-orbites sont deux à deux distinctes. Cela permet d'appliquer la proposition 4.6, d'où: pour tout $n \in \mathbf{N}$, il n'existe qu'un nombre fini d'indices n' tels que $\iota_f(\Gamma) \cdot g_n \cdot K'/K' = \iota_f(\Gamma) \cdot g_{n'} \cdot K'/K'$. Ainsi dans la suite des $\iota_f(\Gamma) \cdot g_{n'} \cdot K'/K'$, donc aussi des $\iota_{\mathbf{R}}(\Gamma')\backslash\iota_{\mathbf{R}}(\Gamma') \cdot G({\iota_{\mathbf{R}}} \circ {\iota_f}^{-1})(g_n) \cdot \iota_{\mathbf{R}}(\Gamma)$, même si les termes ne sont pas deux à deux distincts, il n'y a pas de sous-suite constante.

C'est pourquoi on peut tout de même appliquer la théorème 5.1 à l'action du groupe arithmétique $\iota_{\mathbf{R}}(\Gamma)$ sur $\iota_{\mathbf{R}}(\Gamma')\backslash \mathrm{G}(\mathbf{R})^+$. On conclut donc à l'équidistribution des ensembles E_n de l'énoncé pour la probabilité $G(\mathbf{R})^+$-invariante dans $G(\mathbf{Q})\backslash G(\mathbf{Q}) \cdot G(\mathbf{R})^+ \cdot K'/K'$. □

6 Démonstration

Démontrons finalement le théorème 2.1. Il sera fait usage des énoncés 5.4, 5.2, 3.1, 3.3 et 3.6.

Soit L un corps de type fini contenant ζ_N et contenu dans $\mathbf{C}$, et soit $(z_n)_{n\in\mathbf{N}}$ une suite de points de $Y(N)(\mathbf{C})$ telle que dans l'énoncé. Pour tout $n \in \mathbf{N}$,

soit (E_n, β_n) une courbe elliptique complexe avec structure complète de niveau N représentant le point z_n. Par hypothèse, les courbes E_n sont deux à deux non isomorphes, mutuellement isogènes, sans multiplication complexe, et définissables sur la fermeture algébrique de L dans $\mathbf{C}$.

Fixons $(E, \beta) := (E_0, \beta_0)$ et notons $(P, Q) = (\beta(1,0), \beta(0,1))$. Soit (E_K, β_K) un modèle de (E, β) sur une extension finie de L contenue dans $\mathbf{C}$. Lorsque E est donnée par une équation de Weierstraß $Y^2 = X^3 + aX + b$ à coefficients a et b algébriques sur L, il suffit de prendre pour K l'extension

$$L(a, b, X(P), X(Q), Y(P), Y(Q))/L$$

de L engendré par les coefficients a et b ainsi que les coordonnées de P et Q. C'est une extension finie de L.

Dès lors $\boldsymbol{\mathcal{G}al}(\mathbf{C}/K)$ est un sous-groupe d'indice fini de $\boldsymbol{\mathcal{G}al}(\mathbf{C}/L)$. On applique alors le lemme 5.4 pour $X = Y(N)(\mathbf{C})$, $\mathcal{G} = \boldsymbol{\mathcal{G}al}(\mathbf{C}/L)$ et $\mathcal{H} = \boldsymbol{\mathcal{G}al}(\mathbf{C}/K)$. On en déduit qu'il suffit d'obtenir le résultat d'équidistribution pour des orbites de $\boldsymbol{\mathcal{G}al}(\mathbf{C}/K)$ plutôt que $\boldsymbol{\mathcal{G}al}(\mathbf{C}/L)$. On pourra donc supposer que $K = L$.

Comme les orbites $\boldsymbol{\mathcal{G}al}(\mathbf{C}/L)\cdot z_n$ sont finies et que les points z_n sont supposés distincts, on pourra, quitte à extraire, supposer que les orbites $\boldsymbol{\mathcal{G}al}(\mathbf{C}/L) \cdot z_n$ sont deux à deux distinctes, c'est-à-dire disjointes.

On se fixe une base de $\hat{T}(E)$ relevant β, de sorte que l'on a, suivant 3.1, une identification de $\mathrm{Isog}_{N,\zeta_N}$ avec $\mathbf{Q}^\star\backslash\mathrm{GL}(2,\mathbf{Q})\mathrm{GL}(2)[N\hat{\mathbf{Z}}]/\mathrm{GL}(2)[N\hat{\mathbf{Z}}]$. D'après la proposition 3.3, et moyennant le choix d'un modèle pour (E, β), on a même un morphisme $\rho : \boldsymbol{\mathcal{G}al}(\mathbf{C}/L) \to \mathrm{GL}(2, \hat{\mathbf{Z}})$.

On souhaite appliquer la proposition 5.2 aux orbites de l'action de $\boldsymbol{\mathcal{G}al}(\mathbf{C}/L)$ sur $\mathrm{Isog}_{N,\zeta_N}$. On prend pour G le $\mathbf{Q}$-groupe algébrique linéaire PGL(2). C'est bien un groupe $\mathbf{Q}$-simple de type non compact. On prendra pour K' le sous groupe compact ouvert $\mathrm{PGL}(2)[N\hat{\mathbf{Z}}]$. Quant à K, ce sera l'image de $\rho(\boldsymbol{\mathcal{G}al}(\mathbf{C}/L))$ dans $\mathrm{PGL}(2, \hat{\mathbf{Z}})$. D'après 3.3, c'est un sous-groupe compact ouvert.

Le morphisme quotient $\mathrm{GL}(2) \to \mathrm{PGL}(2)$ induit une application

$$\mathbf{Q}^\star\backslash\mathrm{GL}(2, \mathbf{A}_f)/\mathrm{GL}(2)[N\hat{\mathbf{Z}}] \to G(\mathbf{A}_f)/G(\hat{\mathbf{Z}}).$$

Comme on a $\mathbf{A}_f^\star \cap \mathrm{GL}(2, \mathbf{Q}) = \mathbf{Q}^\star$, celle-ci est injective sur le sous-ensemble $\mathbf{Q}^\star\backslash\mathrm{GL}(2,\mathbf{Q})\mathrm{GL}(2)[N\hat{\mathbf{Z}}]/\mathrm{GL}(2)[N\hat{\mathbf{Z}}]$. Elle identifie par conséquent $\mathrm{Isog}_{N,\zeta_N}$ avec l'ensemble $G(\mathbf{Q})K'/K'$ considéré dans la proposition 5.2. Considérons la suite des orbites, supposées distinctes, $\boldsymbol{\mathcal{G}al}(\mathbf{C}/L) \cdot z_n$ de $\boldsymbol{\mathcal{G}al}(\mathbf{C}/L)$ dans $\mathrm{Isog}_{N,\zeta_N}$, où n décrit $\mathbf{N}$. Elles s'identifient à des orbites deux à deux distinctes de K dans $G(\mathbf{Q})K'/K'$. De plus, $G(\mathbf{R})$ étant connexe, on a $G(\mathbf{R})^+ = G(\mathbf{R})$, et donc $G(\mathbf{Q})^+ = G(\mathbf{Q})$. Par conséquent, les orbites de K dans $G(\mathbf{Q})K'/K'$ sont bien de la forme $K \cdot g_n K'$, où $g_n \in G(\mathbf{Q})^+$.

On a ainsi vérifié toutes les hypothèses nécessaire à l'application de la proposition 5.2 aux orbites de K dans $G(\mathbf{Q})K'/K'$ correspondant aux orbites $\boldsymbol{\mathcal{G}al}(\mathbf{C}/L)\cdot z_n$. On en déduit que ces orbites s'équidistribuent dans l'espace

$$G(\mathbf{Q})\backslash G(\mathbf{Q})\cdot G(\mathbf{R})\cdot K'/K' \simeq \Gamma(N)\backslash G(\mathbf{R})$$

pour la mesure-$G(\mathbf{R})$ invariante à gauche.

Or, d'après la proposition 3.6, en composant l'application

$$\mathrm{Isog}_{N,\zeta_N} \to \Gamma(N)\backslash \mathrm{G}(\mathbf{R})$$

ci-dessus par l'application $\mathrm{PGL}(2,\mathbf{R}) \to Y(N)(\mathbf{C})$ indiquée, on retrouve l'inclusion de $\mathrm{Isog}_{N,\zeta_N}$ dans $Y(N)(\mathbf{C})$. Mais l'application par laquelle on compose envoie la mesure invariante de $\Gamma(N)\backslash \mathrm{G}(\mathbf{R})$ vers la mesure hyperbolique de $Y(N)(\mathbf{C})$. Par conséquent les orbites de $\boldsymbol{\mathcal{G}al}(\mathbf{C}/L)$ dans $\mathrm{Isog}_{N,\zeta_N}$ s'équidistribuent non seulement dans $\Gamma(N)\backslash \mathrm{G}(\mathbf{R})$, mais aussi dans $Y(N)(\mathbf{C})$, ce qui termine la démonstration du théorème principal.

Références

[1] Nelo D. ALLAN : The problem of the maximality of arithmetic groups. *In Algebraic Groups and Discontinuous Subgroups (Proc. Sympos. Pure Math., Boulder, Colo., 1965)*, pages 104–109. Amer. Math. Soc., Providence, R.I., 1966.

[2] Armand BOREL : Some finiteness properties of adele groups over number fields. *Inst. Hautes Études Sci. Publ. Math.*, (16):5–30, 1963.

[3] Armand BOREL : Density and maximality of arithmetic subgroups. *J. Reine Angew. Math.*, 224:78–89, 1966.

[4] Laurent CLOZEL, Hee OH et Emmanuel ULLMO : Hecke operators and equidistribution of Hecke points. *Invent. Math.*, 144(2):327–351, 2001.

[5] Pierre de la HARPE : *Topics in geometric group theory*. Chicago Lectures in Mathematics. University of Chicago Press, Chicago, IL, 2000.

[6] Pierre DELIGNE : Preuve des conjectures de Tate et de Shafarevitch (d'après G. Faltings). *Astérisque*, (121-122):25–41, 1985. Seminar Bourbaki, Vol. 1983/84.

[7] Pierre DELIGNE et Michael RAPOPORT : Les schémas de modules de courbes elliptiques. *In Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 143–316. Lecture Notes in Math., Vol. 349. Springer, Berlin, 1973.

[8] W. Duke : Hyperbolic distribution problems and half-integral weight Maass forms. *Invent. Math.*, 92(1):73–90, 1988.

[9] Alex Eskin et Hee Oh : Ergodic theoretic proof of equidistribution of Hecke points. *Ergodic Theory Dynam. Systems*, 26(1):163–167, 2006.

[10] G. Faltings : Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983.

[11] James E. Humphreys : *Arithmetic groups*, volume 789 de *Lecture Notes in Mathematics*. Springer, Berlin, 1980.

[12] Nicholas M. Katz et Barry Mazur : *Arithmetic moduli of elliptic curves*, volume 108 de *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1985.

[13] Serge Lang : *Elliptic functions*, volume 112 de *Graduate Texts in Mathematics*. Springer-Verlag, New York, second édition, 1987. With an appendix by J. Tate.

[14] Dave Witte Morris : Introduction to arithmetic groups. `http://people.uleth.ca/~dave.morris`.

[15] Shahar Mozes et Nimish Shah : On the space of ergodic invariant measures of unipotent flows. *Ergodic Theory Dynam. Systems*, 15(1):149–159, 1995.

[16] Arkady Onishchik et Ernest Borisovich Vinberg : *Lie groups and Lie algebras. II*, volume 21 de *Encyclopaedia of Mathematical Sciences*. Springer-Verlag, Berlin.

[17] Richard Pink : A combination of the conjectures of Mordell-Lang and André-Oort. *In Geometric methods in algebra and number theory*, volume 235 de *Progr. Math.*, pages 251–282. Birkhäuser Boston, Boston, MA, 2005.

[18] Vladimir Platonov et Andrei Rapinchuk : *Algebraic groups and number theory*, volume 139 de *Pure and Applied Mathematics*. Academic Press Inc., Boston, MA, 1994. Translated from the 1991 Russian original by Rachel Rowen.

[19] Jean-Pierre Serre : *Abelian l-adic representations and elliptic curves*. McGill University lecture notes written with the collaboration of Willem Kuyk and John Labute. W. A. Benjamin, Inc., New York-Amsterdam, 1968.

[20] Jean-Pierre Serre : Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[21] Jean-Pierre SERRE : *Cours d'arithmétique*. Presses Universitaires de France, Paris, 1995. Quatrième édition.

[22] Goro SHIMURA : *Introduction to the arithmetic theory of automorphic functions*, volume 11 de *Publications of the Mathematical Society of Japan*. Princeton University Press, Princeton, NJ, 1994. Reprint of the 1971 original, Kanô Memorial Lectures, 1.

[23] Joseph H. SILVERMAN : *The arithmetic of elliptic curves*, volume 106 de *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1992. Corrected reprint of the 1986 original.

[24] Joseph H. SILVERMAN : *Advanced topics in the arithmetic of elliptic curves*, volume 151 de *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[25] Lucien SZPIRO et Emmanuel ULLMO : Variation de la hauteur de Faltings dans une classe de $\overline{\mathbf{Q}}$-isogénie de courbe elliptique. *Duke Math. J.*, 97(1):81–97, 1999.

[26] J. TITS : Reductive groups over local fields. *In Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 1*, Proc. Sympos. Pure Math., XXXIII, pages 29–69. Amer. Math. Soc., Providence, R.I., 1979.

[27] WIKIPEDIA : Picard-Fuchs equation. `http://en.wikipedia.org/wiki/Picard-Fuchs_equation`.

RÉPARTITION GALOISIENNE D'UNE CLASSE D'ISOGÉNIE DE COURBES ELLIPTIQUES

par

Rodolphe RICHARD

Résumé. — Nous montrons que dans les composantes géométriques des courbes modulaires associées aux sous-groupes de congruence de PSL(2), il y a équidistribution, vers la probabilité hyperbolique, des orbites sous Galois d'invariants modulaires formés à partir de structures de niveau sur des courbes elliptiques issues d'une même classe d'isogénie.

Abstract. — We show that, in geometrically connected modular curves associated with congruence subgroups of PSL(2), one has equidistribution, towards the hyperbolic probability, of Galois orbits of the modular invariants associated with a level structure on elliptic curves within a given isogeny class.

Hyperbolic Galois distribution of an isogeny class of elliptic curves

Write $Y(1)(\mathbf{C})$ for the space of complex points of the modular curve of level 1. It is the usual j-line and, as such, is naturally defined over $\mathbf{Q}$. Consequently, $Y(1)(\mathbf{C})$ carries an action of $\mathrm{Aut}(\mathbf{C}/\mathbf{Q})$, namely the action on j-invariants as complex numbers. For any algebraic j-invariant one constructs an atomic probability measure $\delta_{\mathrm{Aut}(\mathbf{C}/\mathbf{Q})\cdot j}$ on $Y(1)(\mathbf{C})$, adding a Dirac mass at each conjugate of j, and dividing by $\deg(\mathbf{Q}(j))$. In general, $\delta_{\mathrm{Aut}(\mathbf{C}/\mathbf{Q})\cdot j}$ has no particular property. But for families of algebraic numbers whose Weil height goes to 0, Bilu's theorem assert that $\delta_{\mathrm{Aut}(\mathbf{C}/\mathbf{Q})\cdot j}$ tends to the Haar measure on the unit circle.

Our main result here is an analoguous property for families of invariants that come from elliptic curves within a single isogeny class. In this case, one knows from results of [**9**] that the height of the involved invariants is unbounded.

Theorem 1. — *Let E be a complex elliptic curve without complex multiplication. Let $(j_n)_{n\in\mathbf{N}}$ be a sequence of pairwise distinct algebraic j-invariants. We suppose that for every index n, there exists a complex elliptic curve whose j-invariant equals j_n and which is isogeneous to E.*

Then the sequence $\left(\delta_{\mathrm{Aut}(\mathbf{C}/\mathbf{Q})\cdot j_n}\right)_{n\in\mathbf{N}}$ *is convergent and its limit is the hyperbolic probability measure* μ*. Equivalently, for any bounded and continuous real valued function* $f : Y(N)(\mathbf{C}) \to \mathbf{R}$*,*

$$\frac{1}{[\mathbf{Q}(j_n):\mathbf{Q}]}\sum_{z\in\boldsymbol{\mathcal{G}al}(\mathbf{Q}(j_n)/\mathbf{Q})\cdot j} f(z) \to \mu(f) := \int_{Y(N)(\mathbf{C})} f\mathrm{d}\mu$$

as $n \to +\infty$*.*

In this statement "*hyperbolic probability measure*" means the probability measure deduced from the Poincaré measure by uniformization.

Actually, the result we get is more general, encompassing congruence subgroups of PSL(2), and any ground field of finite type over $\mathbf{Q}$. The hypothesis on complex multiplication is unnecessary, thanks to [**2**]. The following is immediate from the theorem and its application to the (unbounded but positive) function $f : z \mapsto \max\{0; \log|z|\}$.

Corollary 2. — *For such a sequence* $(j_n)_{n\in\mathbf{N}}$*, the degree of* $\mathbf{Q}(j(n))$ *goes to* ∞*, and the archimedean part of the Weil height of* j_n *goes to* $+\infty$ *as* $n \to \infty$*.*

Note that it is the *boundedness* of the local height that prevails at finite places.

This main ingredients of the proof are

1. Serre's open image theorem from [**5**] and [**6**];
2. equidistribution of Hecke orbits for real homogeneous spaces;
3. an adelic variant of 2, which is deduced using finiteness of class numbers for arithmetic groups;
4. the above corollary on the degree of $\mathbf{Q}(j_n)$, which is deduced from 1 and finiteness statements from 3.

The author recently remarked that the proof applies to quaternionic fuchsian groups, replacing Serre's theorem by its extension by Ohta in [**4**].

Énoncé. — Soit N un entier naturel non nul. Fixons le choix, dans $\mathbf{C}$, d'une racine de l'unité, disons $\zeta := \exp(2\pi i/N)$. On considère la courbe modulaire $Y(N)$. C'est une courbe algébrique *affine* et *géométriquement connexe* définie sur $\mathbf{Q}(\zeta)$. L'espace $Y(N)(\mathbf{C})$ de ses points complexes s'identifie au quotient du demi-plan de Poincaré $\mathfrak{H} := \{\tau \in \mathbf{C} | \Im(\tau) > 0\}$ par l'action à gauche du groupe $\Gamma(N)$. La mesure de Poincaré sur $\mathfrak{H}$ détermine une mesure de probabilité μ, que l'on qualifiera d'*hyperbolique*, sur $Y(N)(\mathbf{C})$.

Le schéma $Y(N)$ est l'espace de modules (fin pour $N \geq 3$, grossier pour $N = 1$ ou 2) des courbes elliptiques munies d'une *structure complète de niveau* N *de racine associée* ζ, c'est-à-dire de deux points rationnels de N-torsion P et Q dont l'accouplement de Weil $e(P, Q)$ (normalisé comme en [**8**] III.§8) vaut ζ.

Soit E une courbe elliptique complexe. Considérons une suite $(E_n)_{n\in\mathbf{N}}$ de courbes elliptiques complexes toutes isogènes à E. On choisit, pour chaque n, une structure

complète de niveau N et de racine ζ sur E_n, que l'on notera β_n. À chaque couple (E_n, β_n) correspond un point de $Y(N)(\mathbf{C})$. Notons-le z_n.

Soit L un corps de type fini sur $\mathbf{Q}$ sur lequel E admet un modèle. Alors, pour chaque n, l'orbite de z_n sous $\mathrm{Aut}(\mathbf{C}/L)$ est finie. On notera $\delta_L(z_n)$ la probabilité sur $Y(N)(\mathbf{C})$ supportée par cette orbite et affectant du même poids chacun des conjugués de z_n. Notre résultat décrit le comportement asymptotique de $\delta_L(z_n)$.

Théorème 1. — *On suppose E sans multiplication complexe. Supposons aussi que l'on ne puisse pas extraire de $(z_n)_{n\in\mathbf{N}}$ une suite constante.*

Alors la probabilité $\delta_L(z_n)$ converge vers la probabilité hyperbolique μ lorsque n tend vers $+\infty$.

Autrement dit, pour toute fonction continue bornée $f : Y(N)(\mathbf{C}) \to \mathbf{R}$,

$$\delta_L(z_n)(f) := \frac{1}{\#\mathrm{Aut}(\mathbf{C}/L)\cdot z_n} \sum_{z\in \mathrm{Aut}(\mathbf{C}/L)\cdot z_n} f(z) \to \mu(f) := \int_{Y(N)(\mathbf{C})} f \mathrm{d}\mu$$

lorsque $n \to +\infty$.

Ce résultat ne rentre pas *a priori* dans le cadre de l'équidistribution des points de petite hauteur. En effet la hauteur de Faltings d'une suite de courbes elliptiques dans une même classe d'isogénie n'est en général pas bornée ([**9**]). L'énoncé analogue, dans le cas où E admet de la multiplication complexe, est lui aussi valide ; dans ce cas, l'hypothèse que les courbes soient isogènes est superflue, d'après un théorème de William Duke ([**2**]).

Notre méthode combine une forme adélique l'*équidistribution des points de Hecke* et les propriétés d'*image ouverte* d'un groupe de Galois agissant sur la torsion de courbes elliptiques.

Classe d'isogénie, Action galoisienne et Uniformisation. — Pour toute courbe elliptique complexe E, on notera $\hat{T}(E)$ son module de Tate profini, et $\hat{V}(E)$ son module de Tate adélique. Ce sont des modules libres de rang 2 sur $\hat{\mathbf{Z}}$ et $\mathbf{A}_f$ respectivement, et ils dépendent fonctoriellement de E. On notera K_N le sous-groupe principal de congruence modulo N de $\mathrm{GL}(2, \hat{\mathbf{Z}})$, et on notera $\mathrm{Aut}(E \otimes \mathbf{Q})$ le groupe des inversibles de l'algèbre $\mathrm{End}(E/\mathbf{C}) \otimes \mathbf{Q}$.

Soit E une courbe elliptique complexe et soit $\varphi : {\mathbf{A}_f}^2 \to \hat{V}(E)$ un isomorphisme $\mathbf{A}_f$-linéaire. Il existe un entier n_φ, une courbe elliptique complexe E_φ, et une isogénie $\pi_\varphi : E_\varphi \to E$ tels que les images de $\hat{T}(\pi_\varphi) : \hat{T}(E_\varphi) \to \hat{T}(E)$ et de $n_\varphi \cdot \varphi$ coïncident dans $\hat{T}(E)$. Il s'ensuit que la correspondance

$$\gamma_\varphi : \hat{\mathbf{Z}}^2 \xrightarrow{n_\varphi\cdot\varphi} \hat{T}(E) \xleftarrow{\hat{T}(\pi_\varphi)} \hat{T}(E_\varphi)$$

est un isomorphisme de $\hat{\mathbf{Z}}^2$ sur $\hat{T}(E_\varphi)$. Cela définit, par passage au quotient, une structure de niveau N sur E_φ, disons $\beta_\phi : (\mathbf{Z}/(N))^2 \longrightarrow E_\varphi[N]$.

La classe d'isomorphisme de $(E_\varphi, \beta_\varphi)$ ne dépend que de φ. On notera ζ_φ la racine de l'unité associée à β_φ, et lorsque $\zeta_\varphi = \zeta$, on notera z_φ le point de $Y(N)(\mathbf{C})$ qui représente $(E_\varphi, \beta_\varphi)$.

Soit $\mathrm{Isom}_\zeta({\mathbf{A}_f}^2, \hat{V}(E))$ l'ensemble des isomorphismes $\mathbf{A}_f$-linéaires φ de ${\mathbf{A}_f}^2$ sur $\hat{V}(E)$ tels que $\zeta_\varphi = \zeta$. Soit aussi $\mathrm{Isog}_\zeta(E)$ le sous-ensemble de $Y(N)(\mathbf{C})$ des invariants modulaires provenant de courbes isogènes à E (munies de structures de racine ζ). Alors l'application $\varphi \mapsto z_\varphi$ de $\mathrm{Isom}_\zeta({\mathbf{A}_f}^2, \hat{V}(E))$ vers $Y(N)(\mathbf{C})$ est bien définie et son image est $\mathrm{Isog}_\zeta(E)$. Cette application est en outre invariante à gauche sous $\mathrm{Aut}(E \otimes \mathbf{Q})$, à droite sous K_N et elle induit une bijection

$$\mathrm{Aut}(E \otimes \mathbf{Q}) \backslash \mathrm{Isom}_\zeta({\mathbf{A}_f}^2, \hat{V}(E))/K_N \to \mathrm{Isog}_\zeta(E).$$

Fixons un modèle de E sur un sous-corps L de $\mathbf{C}$ contenant $\mathbf{Q}(\zeta)$. On en déduit une représentation de $\mathrm{Aut}(\mathbf{C}/L)$ sur $\hat{T}(E)$, puis, par composition, une action à gauche sur $\mathrm{Isom}_\zeta({\mathbf{A}_f}^2, \hat{V}(E))$. Cette action est compatible, via la flèche $\varphi \mapsto z_\varphi$ à l'action à gauche de $\mathrm{Aut}(\mathbf{C}/L)$ sur les $\mathbf{C}$-points de $Y(N)$.

Enfin cette application est « compatible à l'uniformisation » de $Y(N)(\mathbf{C})$, au sens où elle s'inscrit dans un carré commutatif

$$\begin{array}{ccc} \mathrm{Isom}_\zeta({\mathbf{A}_f}^2, \hat{V}(E)) & \longrightarrow & \mathrm{PGL}(2,\mathbf{Q})\backslash\mathrm{PGL}(2,\mathbf{A}) \\ \downarrow & & \downarrow \\ \mathrm{Aut}(E \otimes \mathbf{Q}) \backslash \mathrm{Isom}_\zeta({\mathbf{A}_f}^2, \hat{V}(E))/K_N & \longrightarrow & Y(N)(\mathbf{C}) \end{array}$$

Dans ce diagramme, la flèche supérieure est équivariante *à droite* sous le stabilisateur de $\mathrm{Isom}_\zeta({\mathbf{A}_f}^2, \hat{V}(E))$ dans $\mathrm{GL}(2, \mathbf{A}_f)$. Il est formé des g pour lesquels $\mathbf{dét}(g) \in \mathbf{Q}^\star \cdot (N\hat{\mathbf{Z}})^\star$. La flèche de droite est un quotient par un sous-groupe compact maximal de $\mathrm{PGL}(2, \mathbf{A})$, de la forme $K' \times \mathrm{PSO}(2, \mathbf{R})$. On choisira pour K' le sous-groupe de $\mathrm{PGL}(2, \hat{\mathbf{Z}})$ engendré par le sous-groupe principal de congruence modulo N *et par le tore diagonal*. Dès que $N \geq 3$, ce groupe K' contient *strictement* l'image de K_N dans $\mathrm{PGL}(2, \hat{\mathbf{Z}})$.

Démonstration du théorème, Image ouverte. — On se place dans la situation de l'introduction et sous les hypothèses du théorème. Pour chaque n, on choisit un isomorphisme $\varphi_n \in \mathrm{Isom}_\zeta({\mathbf{A}_f}^2, \hat{V}(E))$ tel que $z_{\varphi_n} = z_n$. On déduit de ce qui précède que l'orbite $\mathrm{Aut}(\mathbf{C}/L) \cdot z_n$ dans $Y(N)(\mathbf{C})$ est l'image de $\mathrm{Aut}(\mathbf{C}/L) \cdot \varphi_n$. Soit $\mathrm{PGL}(2, \mathbf{Q}) \cdot g_n$ l'image de φ_n dans $\mathrm{PGL}(2, \mathbf{Q})\backslash\mathrm{PGL}(2, \mathbf{A})$. D'après la commutativité du diagramme ci-dessus, $\mathrm{Aut}(\mathbf{C}/L) \cdot z_n$ est l'image dans $Y(N)(\mathbf{C})$ d'un ensemble de la forme $\mathrm{PGL}(2, \mathbf{Q}) \cdot K \cdot g_n$ où K est un sous-groupe de $\mathrm{PGL}(2, \hat{\mathbf{Z}})$ déterminé par l'action de $\mathrm{Aut}(\mathbf{C}/L)$ sur $\hat{T}(E)$.

Après avoir déduit du fait suivant que K est ouvert, on montre la propriété d'équidistribution annoncée en appliquant la proposition 2 pour $G = \mathrm{PGL}(2)$.

Proposition 1. — *Soit E une courbe elliptique sans multiplication complexe géométrique définie sur un corps L de type fini sur $\mathbf{Q}$ et contenu dans $\mathbf{C}$. Considérons la représentation ρ de $\mathrm{Aut}(\mathbf{C}/L)$ sur $\hat{T}(E)$.*

Alors l'image de ρ est un sous-groupe d'indice fini du groupe, isomorphe à $\mathrm{GL}(2, \hat{\mathbf{Z}})$, des automorphismes continus du groupe abélien profini $\hat{T}(E)$.

Cela se déduit du théorème de l'image ouverte de Serre ([**5**] et [**6**]) dans le cas où $j(E)$ est algébrique sur $\mathbf{Q}$, et des travaux de Shimura dans le cas où $j(E)$ est transcendant ([**7**]).

Équidistribution adélique et Points de Hecke. — Soit G un groupe algébrique sur $\mathbf{Q}$. On désigne par $G(\mathbf{R})^+$ la composante neutre du groupe de Lie réel associé, et on identifie $G(\mathbf{Q})$ à son image dans $G(\mathbf{A})$ par le plongement diagonal. Soit $G(\mathbf{Q})^+$ l'image inverse de $G(\mathbf{R})^+$ par le morphisme $G(\mathbf{Q}) \to G(\mathbf{R})$ et soit $\iota_f(\mathbf{Q})$ l'image de $\mathbf{Q}$ dans l'anneau $\mathbf{A}_f$. Alors $G(\iota_f(\mathbf{Q}))^+$ désignera l'image de $G(\mathbf{Q})^+$ dans $G(\mathbf{A}_f)$ et $\overline{G(\iota_f(\mathbf{Q}))^+}$ son adhérence dans $G(\mathbf{A}_f)$. Le résultat suivant utilise la propriété d'équidistribution des points de Hecke (voir [**1**] ou [**3**]).

Proposition 2. — *Soit G un groupe algébrique linéaire $\mathbf{Q}$-simple connexe de type non compact. Soient K et K' deux sous-groupes compacts et ouverts de $G(\mathbf{A}_f)$. On désigne par μ la probabilité $G(\mathbf{R})^+$-invariante sur le $G(\mathbf{R})^+$-espace homogène à droite connexe $\mathbf{X} := G(\mathbf{Q})\backslash G(\mathbf{Q}) \cdot G(\mathbf{R})^+ \cdot K'/K'$.*

Soit $(g_n)_{n\in\mathbf{N}}$ une suite de $\overline{G(\iota_f(\mathbf{Q}))^+}$ sans valeur d'adhérence dans $G(\mathbf{A}_f)$. Considérons les sous-ensembles de $G(\mathbf{A}_f)$ suivants.

$$E_n = (K \cdot g_n) \cap \left(\overline{G(\iota_f(\mathbf{Q}))^+} \cdot K'\right)$$

Alors, pour toute fonction continue et bornée $f : \mathbf{X} \to \mathbf{R}$,

$$\frac{\displaystyle\sum_{x \in G(\mathbf{Q})\backslash G(\mathbf{Q})\cdot E_n \cdot K'/K'} f(x)}{\#G(\mathbf{Q})\backslash G(\mathbf{Q}) \cdot E_n \cdot K'/K'} \text{ tend vers } \int_{\mathbf{X}} f \mathrm{d}\mu \text{ lorsque } n \to +\infty.$$

Dernières remarques. — **1.** L'énoncé de [**3**] utilise comme hypothèse que les orbites considérées doivent avoir un cardinal (le « degré » des points considérés) de plus en plus grand. Pour des réseaux arithmétiques, cette hypothèse est automatiquement vérifiée. Ce sont des propriétés de finitude que nous déduisons des résultats généraux d'A. Borel sur l'arithmétique des groupes semi-simples de type non-compact. Dans le cas qui nous intéresse, celui des courbes modulaires $Y(N)(\mathbf{C})$, cela se traduit, par l'énoncé suivant. On notera que cet énoncé, qui n'est pas sans rappeler le théorème de Shafarevich ([**5**]), est un corollaire du théorème 1.

Proposition 3. — *Soit E une courbe elliptique définie sur un corps L de type fini et contenu dans $\mathbf{C}$. Alors il n'existe, à $\mathbf{C}$-isomorphisme près qu'un nombre fini de courbes elliptiques complexes définissables sur L et $\mathbf{C}$-isogènes à E.*

2. Nous avons restreint l'énoncé du théorème aux courbes modulaires $Y(N)$. Mais notre résultat s'étend tel quel aux courbes modulaires géométriquement connexes associées aux sous-groupes de congruence de $\Gamma(1)$, vu que ces dernières sont recouvertes par les courbes $Y(N)$. On peut également adapter l'énoncé au cas non connexe. Les mesures limites seront alors les moyennes arithmétiques de probabilités associées aux composantes géométriquement connexes issues d'une même composante connexe.
3. Plus récement, l'auteur a remarqué que ce résultat s'étend aux courbes de Shimura associées à des algèbres de quaternions non déployées. Les courbes elliptiques sont alors remplacées par des surfaces abéliennes à multiplication quaternionique, auxquelles M. Ohta ([**4**]) a étendu la proposition 1.

Références

[1] Laurent Clozel, Hee Oh et Emmanuel Ullmo, *Hecke operators and equidistribution of Hecke points*, Invent. Math. **144** (2001), pp.327–351.

[2] William Duke, *Hyperbolic distribution problems and half-integral weight Mass forms*, Invent. Math. **92** (1988).

[3] Alex Eskin et Hee Oh, *Ergodic theoretic proof of equidistribution of Hecke points*, To appear in Erg. The. and Dyn. Sys.

[4] Masami Ohta, *On ℓ-adic representations of Galois groups obtained from certain two-dimensional abelian varieties*, J. Fac. Sci. Univ. Tokyo Sect. IA Math., Vol. **21** (1974).

[5] Jean-Pierre Serre, *Abelian ℓ-Adic Representations and Elliptic Curves*, W.A. Benjamin, Inc. (1968).

[6] Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), *no 4*. pp. 258–331.

[7] Goro Shimura, *Introduction to the arithmetic theory of automorphic forms*, Kanô Memorial Lectures, *no. 1* aux Publications of the Mathematical Society of Japan, *no. 11*, Princeton University Press, 1971.

[8] Joseph H. Silverman, *The Arithmetic of elliptic curves*, Graduate Texts in mathematics, *no 106.*

[9] Lucien Szpiro, Emmanuel Ullmo, *Variation de la hauteur de Faltings dans une classe de $\overline{\mathbb{Q}}$–isogénie de courbe elliptique*, Duke Math. J., **97**, *no 1*, (1999), pp. 81–97.

Rodolphe Richard

ÉQUIDISTRIBUTION ET VARIÉTÉS DE SHIMURA

par

Rodolphe RICHARD

Table des matières

Introduction 3
Mesures et Actions de groupe 4

Partie I. Variétés de Shimura 7
1. Quotients arithmétiques 7
2. Données de Shimura connexes 11
3. Variétés de Shimura complexes 15
4. Modèles canoniques, Action de Galois et Orbites de Hecke 18

Partie II. Propriétés d'équidistribution 20
5. Une Propriété de finitude sur les groupes arithmétiques 20
6. Équidistribution des points de Hecke 21
7. Cas adélique 23

Partie III. Répartition hyperbolique d'orbites de Hecke et d'orbites de Galois 24
8. Mesures hyperboliques 24
9. Équidistribution des points de Hecke 24
10. Équidistribution galoisienne 24
11. Espaces de modules de variétés abéliennes 25
Références 26

Introduction

Cette note apporte quelques précisions quant à la conjecture 1.6 de l'article [**Pin05**] de R. Pink. Plus particulièrement nous étendons les théorèmes 7.5 et 7.6 de [**Pin05**] sur deux points.

Le premier point est que nous montrons une forme plus fine de la conjecture 1.6 dans les cas considérés. Il s'agit d'une forme plus fine même que celle évoquée par la remarque 7.7 (b) de [**Pin05**] car nous déduisons une propriété d'équidistribution.

En outre, nous nous basons sur une variante du théorème principal [**COU01**] qui optimise quelques hypothèses. Nous répondons en cela à la remarque 7.7 (c) de [**Pin05**], et prenons également en compte les groupes réductifs anisotropes sur $\mathbf{Q}$.

Un théorème de M. Ohta [**Oht74**] montre que les hypothèses de l'énoncé 11.1 sont satisfaites dans le contexte des surfaces abéliennes à multiplication quaternionique et sans multiplication complexe. Sont ainsi couverts tous les cas de courbes de Shimura sur un corps de nombres, ce qui répond à une remarque de [**Ric09a**].

Notre exposé fera librement usage du langage des variétés de Shimura, au sens de P. Deligne, décrites sous forme adélique. Les notations seront celles de [**Del79**]. Nous rappelons les faits dont nous ferons usage et précisons la terminologie utilisée.

Ce texte fait suite à [**Ric09a**] où l'on trouvera traité en détail le cas des espaces de modules de courbes elliptiques. Il est organisée comme suit. Dans une première partie nous rappelons quelques faits sur les variétés de Shimura complexes « en niveau infini ». La section qui suit reformule dans ce contexte nous réexprimons la propriété d'équidistribution des points de Hecke, sous forme adélique. Ensuite nous rappelons quelques faits sur les modèles canoniques des variétés de Shimura et l'action galoisienne sur une orbite de Hecke, ce qui nous permet dans la section suivante d'énoncé la forme générale du résultat principal. Enfin nous décrivons les conséquences de ce résultat dans le contexte plus familier des espaces de modules de variétés abéliennes avec polarisation et structure de niveau.

Mesures et Actions de groupe

Cette section précise les notions de mesure et de convergence utilisées et rappelle les propriétés fondamentales des mesures de Haar, des mesures invariantes, des mesures quotients, et la notion de réseau.

Mesures et Convergence. — Les seules mesures que nous aurons à considérer seront des *mesures de Radon* sur des espaces boréliens localement compacts. Nous entendons par là une mesure borélienne qui s'obtient par le théorème de représentation de Riesz, sous la forme donnée par [**Rud87**] 2.14, à partir d'une fonctionnelle positive sur les fonctions à support compact. Ces mesures sont notamment *boréliennes*, *réelles*, *positives*, *localement finies*, *extérieurement régulières* et *localement intérieurement régulières*. Dorénavant nous utiliserons le terme « mesure » pour désigner une mesure de Radon. La seule différence avec la convention de [**Bou63**], chapitre VII, est que nos mesures sont réelles et positives, plutôt que réelles signées, voire complexes.

La *masse* d'une mesure μ sur un espace topologique localement compact X désigne la valeur, dans $\mathbf{R}_{\geq 0} \cup \{+\infty\}$, de $\mu(X)$. La mesure μ est dite *bornée* si sa masse est finie, auquel cas toute fonction réelle borélienne bornée sur X est intégrable (relativement à μ). Une *mesure de probabilité*, ou *probabilité*, désignera une mesure de masse 1.

On dit d'une suite de *mesures* $(\mu_n)_{n\in\mathbf{N}}$ (resp. une suite de *mesures bornées*) sur X qu'elle converge *vaguement* (resp. *étroitement*) vers une mesure (resp. une mesure bornée) μ si pour toute *fonction continue à support compact* (resp. *fonction continue bornée*) f sur X, la suite numérique $(\mu_n(f))_{n\in\mathbf{N}}$ converge vers $\mu(f)$. La convergence étroite implique la convergence vague.

La limite d'une suite de mesures de probabilités convergeant *étroitement* est nécessairement de masse 1, c.-à-d. une probabilité. Il se peut toutefois qu'une suite de probabilités converge *vaguement* vers une mesure de masse strictement inférieure, par exemple la suite des masses de Dirac aux entiers naturels. En termes imagés, on dit qu'il y a « perte de masse à l'infini ». En revanche pour qu'une suite de mesures de probabilités converge étroitement vers une probabilité donnée, il suffit qu'elle converge vaguement vers cette probabilité.

En d'autre termes, sur l'espace des probabilités les convergences étroite et vague sont équivalentes ; cet espace est fermé dans celui des mesures pour la convergence étroite, mais pas nécessairement pour la convergence vague.

Invariance, Mesure de Haar, Module. — Soit G un groupe et soit X un espace localement compact sur lequel G agit, à gauche ou à droite, par homéomorphismes. Alors l'action de G se transporte à l'algèbre des fonctions à support compact sur X et, par suite, aux mesures (de Radon). Comme la masse est un invariant de cette action de G, l'espace des probabilités est stable. Une mesure sur X sera dite *invariante* si elle est stable par image directe par l'action de tout élément de G.

Soit G un groupe localement compact. Alors on peut faire agir continûment G sur son espace sous-jacent à gauche ou à droite, par translations ou par conjugaisons (à gauche et à droite resp.). On appelle *mesure de Haar* à gauche (resp. à droite) sur G une mesure non nulle sur G qui est invariante pour l'action par translations à gauche (resp. à droite).

L'opération d'image directe par l'inversion $g \mapsto g^{-1}$ échange mesures de Haar à droite et à gauche. D'après [**Bou63**] VI, Théorème 1, pour tout groupe localement compact G il existe une mesure de Haar à gauche et les mesures de Haar à gauche sur G sont toutes proportionnelles (d'un facteur réel positif et inversible).

L'opération $\phi_\star$ d'image directe par un automorphisme bicontinu ϕ de G stabilise la famille des mesures de Haar à gauche et celle des mesures de Haar à droite. Cette opération commute à la multiplication scalaire : elle agit sur chacune de ces familles par un facteur. Ce facteur ne dépend pas de la famille car tout automorphisme commute à l'inversion. On l'appelle module de ϕ *l'inverse* de ce facteur ([**Bou63**], Définition 4). C'est aussi le facteur par lequel agit l'opération d'*image inverse* par ϕ. Un antiautomorphisme échange mesures de Haar à droite et à gauche.

Remarquons que sur les mesures de Haar à droite (resp. à gauche) l'action par conjugaison à gauche (resp. à droite) est la même que celle par translations à gauche (resp. à droite).

L'*Intégration* de N. Bourbaki ([**Bou63**], VII 3. Définition 3) définit le *module* du groupe G comme la fonction réelle positive, notée $\Delta_G : G \to \mathbf{R}_+^\times$ qui à tout élément g associe le module de l'automorphisme intérieur de conjugaison *à gauche*. Ainsi $\Delta_G(g)$ est le facteur par lequel agit l'image *inverse* par la conjugaison à gauche par g, c'est-à-dire l'image directe par la conjugaison à *droite*.

Le module Δ_G de G est un morphisme continu de G vers $\mathbf{R}^\times$. On dit que G est *unimodulaire* si son module est une constante, nécessairement égale à 1.

Exemples. — Si k est le corps local $\mathbf{R}$ (resp. $\mathbf{C}$, resp. $\mathbf{Q}_p$, resp. l'anneau des adèles $\mathbf{A}_\mathbf{Q}$), alors les autmorphismes du groupe additif de k sont les homothéties de rapport inversible, et le module d'une homothétie $\mu \mapsto \lambda \cdot \mu$ de rapport inversible λ est la valeur absolue $|\lambda|$ de λ (resp. son carré $|\lambda|^2$, resp. la valeur absolue p-adique $|\lambda|_p$, resp. le module de l'idèle λ.) Par exemple, pour $\mathbf{R}$, considérant $x \mapsto x' = \lambda x$, la mesure $\left|dx'\right|$ a pour image inverse $\left|dx'\right| = |\lambda| \cdot |dx|$.

Pour λ dans $k^\times$, appelons *module de* λ le module de l'homothétie de k de rapport λ. Le module d'un automorphisme k-linéaire de k^n est le module de son déterminant : comme le module vaut l'unité sur les commutateurs, on se ramène aux automorphismes diagonalisables.

Le groupe linéaire $GL(n,k)$ est unimodulaire. En revanche la fonction module du groupe *affine* de k^n est donnée par le module du déterminant de la partie linéaire. Pour $n = 1$, le groupe affine, bien que résoluble, n'est pas unimodulaire.

Plus généralement, soit G est un groupe algébrique linéaire sur k. Munissons $G(k)$ de la topologie métrique ou adélique induite par un plongement fermé $G \to SL(N)$. Le module de $G(k)$ est le module de l'inverse du déterminant de la représentation adjointe ([**Bou**] §16.). L'unimodularité de G revient à la nullité de la somme des poids de l'action d'un (tore déployé maximal d'un) sous-groupe de Levi sur le radical unipotent. En particulier si G est réductif ou unipotent, $G(k)$ est unimodulaire.

Remarquons que G est unimodulaire s'il contient une partie borélienne invariante par conjugaison de mesure finie et non nulle (cf. [**Bou63**], Proposition 3). En particulier les groupes localement compacts qui sont *abéliens*, *discrets* ou *compacts* sont unimodulaires.

Comme le but de Δ_G ne contient pas de sous-groupe simple ou compact non nul, le noyau de Δ_G contient tout sous-groupe simple et tout sous-groupe compact de G. Le noyau de Δ_G contient aussi le centre de G et le sous-groupe dérivé de G.

Réseaux. — Soit G un groupe localement compact, et soit Γ un sous-groupe discret de G. Alors Γ admet une mesure de Haar (à droite et à gauche) canonique : la mesure de comptage. Considérons, sur $\Gamma\backslash G$, la mesure quotient μ d'une de Haar à gauche μ_G de G par la mesure de Haar de Γ. On dit que Γ est un *réseau* si μ est bornée. Quitte à faire agir l'inversion, on vérifie que cette définition se confond avec la définition analogue où l'on considère le quotient à droite G/Γ.

Le groupe G agit à droite, par translations, sur $\Gamma\backslash G$; l'effet induit sur μ_G est donné par g : $\mu_G \mapsto \Delta_G(g)\mu_G$. Comme $\mu \cdot g(\Gamma\backslash G) = \mu(\Gamma\backslash G \cdot g) = \mu(\Gamma\backslash G)$, cette action préserve la masse de μ, qui est finie (et non nulle). Par conséquent le module Δ_G est constant.

Il en ressort que si G admet un réseau, alors G est unimodulaire.

Un sous-groupe discret Γ de G tel que le quotient $\Gamma\backslash G$ est automatiquement un réseau. Selon les auteurs, on parle alors de réseau *uniforme*, ou *cocompact*.

PARTIE I
VARIÉTÉS DE SHIMURA

Dans cette partie nous rappelons quelques définitions et quelques faits concernant les *quotients arithmétiques*, le langage de P. Deligne des *variétés de Shimura*, suivant [**Del79**], et leur modèles. Nous précisons ainsi les conventions de notation et de terminologie utilisées. Le théorème principal et sa démonstration n'utiliseront de cette partie que

- la description adélique des points complexes d'une variété de Shimura de niveau infini (en (1)) ;
- la description de ses composantes géométriques (en 3.5) ;
- la définition de l'action de Hecke, et des orbites de Hecke (en 3.3) ;
- la rationalité de l'action de Hecke sur un modèle, et plus particulièrement la conséquence (5).

L'autre ingrédient de notre résultat principal, la reformulation de la propriété d'équidistribution des points de Hecke, fera l'objet de la partie II.

1. Quotients arithmétiques

1.1. Notion de sous-groupe arithmétique. — Selon le contexte, qualifier un sous-groupe d'*arithmétique* peut recouvrir plusieurs notions. Nous précisons ici la terminologie utilisée.

1.1.1. Soit G est un groupe algébrique linéaire sur $\mathbf{Q}$. Suivant A. Borel, dans [**Bor69**] (7.11, voir aussi 7.14 Remarque), on appelle *sous-groupe arithmétique de* $G(\mathbf{Q})$ un sous groupe de $G(\mathbf{Q})$ tel qu'il existe

- une représentation *fidèle* $\rho : G \to GL(V)$ de degré fini et définie sur $\mathbf{Q}$,
- et un réseau R de $V(\mathbf{R})$ contenu dans $V(\mathbf{Q})$

tels que Γ soit commensurable au stabilisateur de R dans $G(\mathbf{Q})$. D'après [**Bor69**] 7.13, on peut fixer la représentation ρ, pourvu qu'elle soit fidèle, et le réseau R, pourvu qu'il soit formé de points rationnels. Par conséquent les sous-groupes arithmétiques de $G(\mathbf{Q})$ sont tous commensurables à un même sous-groupe. En particulier ils sont commensurables deux-à-deux. Remarquons qu'étant donné G, il existe toujours au moins un sous-groupe arithmétique de $G(\mathbf{Q})$.

Cette notion de sous-groupe arithmétique est invariante par isogénie. Plus précisément, soit $\phi : G \to G'$ une isogénie et notons $\phi_{\mathbf{Q}} : G(\mathbf{Q}) \to G'(\mathbf{Q})$ le morphisme de groupe abstraits correspondant. Alors d'après [**BHC62**], Corollaire du Théorème 2 (voir [**Bor69**] 8.9), l'image par $\phi_{\mathbf{Q}}$ d'un sous-groupe arithmétique est encore un sous-groupe arithmétique, et réciproquement, comme nous le montrons ci-dessous, l'image inverse par $\phi_{\mathbf{Q}}$ d'un sous-groupe arithmétique de $G'(\mathbf{Q})$ est un sous-groupe arithmétique de $G(\mathbf{Q})$.

Démonstration. — Comme deux sous-groupes arithmétiques sont commensurables et que $\phi_{\mathbf{Q}}$ est de degré fini, il suffit d'établir l'arithméticité de l'image inverse pour un seul exemple de sous-groupe arithmétique de $G'(\mathbf{Q})$. Soit Γ un sous-groupe arithmétique de $G(\mathbf{Q})$. D'après [**Bor69**] 8.9, son image $\phi_{\mathbf{Q}}(\Gamma)$ est un exemple de sous-groupe

arithmétique de $G'(\mathbf{Q})$. Or l'image inverse $\overset{-1}{\phi}_{\mathbf{Q}}\left(\phi_{\mathbf{Q}}(\Gamma)\right)$ est un sous-groupe de $G(\mathbf{Q})$ qui contient Γ comme sous-groupe d'indice au plus $\#\ker(\phi_{\mathbf{Q}})$. Cette image inverse est donc commensurable avec Γ, et c'est par conséquent un sous-groupe arithmétique de $G(\mathbf{Q})$. □

En particulier, si G est semi-simple la représentation adjointe induit une isogénie de G sur son image, disons G^{ad}. Par conséquent un sous-groupe de $G(\mathbf{Q})$ est arithmétique si et seulement si son image par la représentation adjointe est un sous-groupe arithmétique de $G^{\mathrm{ad}}(\mathbf{Q})$.

1.1.2. Plus généralement, si G est un groupe algébrique linéaire sur $\mathbf{Q}$, nous appellerons *sous-groupe arithmétique de* $G(\mathbf{R})$ *relativement à* G tout sous-groupe de $G(\mathbf{R})$ commensurable à un sous-groupe arithmétique de $G(\mathbf{Q})$.

De tels sous-groupes ne sont pas nécessairement contenus dans $G(\mathbf{Q})$. Toutefois, lorsque le théorème de densité de Borel s'applique, leur image dans $G^{\mathrm{ad}}(\mathbf{R})$ est contenue dans $G^{\mathrm{ad}}(\mathbf{Q})$ ([**All66**]).

Soit Γ un sous-groupe arithmétique de $G(\mathbf{R})$ relativement à G, notons $\overline{\Gamma}$ son adhérence dans G, et notons G^1 l'intersection des noyaux des caractères définis sur $\mathbf{Q}$ de G. D'après le théorème de densité de Borel, la composante neutre de $\overline{\Gamma}^0$ de $\overline{\Gamma}$ est le plus petit sous-groupe algébrique *distingué* et *défini sur* $\mathbf{Q}$ de G tel que $G(\mathbf{R})/\overline{\Gamma}^0(\mathbf{R})$ soit compact. En particulier si G est semi-simple et si tout quasi-facteur H de G défini sur $\mathbf{Q}$ est isotrope (c.-à-d. que le groupe $H(\mathbf{R})$ n'est pas compact), alors tout sous-groupe arithmétique de $G(\mathbf{R})$ relativement à G est Zarisiki dense dans G.

1.1.3. Lorsque G est un sous-groupe algébrique linéaire sur $\mathbf{R}$, un *sous-groupe arithmétique de* $G(\mathbf{R})$ désignera un sous-groupe arithmétique de $G(\mathbf{R})$ relativement à un modèle quelconque de G sur $\mathbf{Q}$.

Cette notion n'est en général pas stable par image directe par un épimorphisme (défini sur $\mathbf{R}$) de groupe algébriques réels (sauf si bien sûr l'épimorphisme et les sous-groupe arithmétique sont définis sur $\mathbf{Q}$ relativement à un même modèle.)

Soit Γ un sous-groupe arithmétique de $G(\mathbf{R})$ relativement à un modèle $G_{\mathbf{Q}}$. Notons $\overline{\Gamma}$ l'adhérence de Zariski de Γ dans G, et $\overline{\Gamma}^0$ la composante neutre de $\overline{\Gamma}$. Alors $\overline{\Gamma}^0$ est défini sur $\mathbf{Q}$ relativement au modèle $G_{\mathbf{Q}}$, et le modèle correpondant de $\overline{\Gamma}^0$ ne dépend pas de $G_{\mathbf{Q}}$, pourvu que Γ soit arithmétique relativement à $G_{\mathbf{Q}}$. Notons $\overline{\Gamma}^0_{\mathbf{Q}}$ ce modèle, uniquement déterminé par Γ, de $\overline{\Gamma}^0$. Réciproquement les modèles G' de G sur $\mathbf{Q}$ relativement auxquels Γ est un sous-groupe arithmétique sont ceux relativement auxquels $\overline{\Gamma}^0$ est défini sur $\mathbf{Q}$ et qui induisent sur $\overline{\Gamma}^0$ le modèle $\overline{\Gamma}^0_{\mathbf{Q}}$. Enfin deux sous-groupes arithmétiques Γ et Γ' de $G(\mathbf{R})$ sont commensurables si et seulement si $\overline{\Gamma}^0_{\mathbf{Q}} = \overline{\Gamma'}^0_{\mathbf{Q}}$, c'est-à-dire si $\overline{\Gamma}^0 = \overline{\Gamma'}^0$ et si Γ et Γ' induisent le même modèle sur $\overline{\Gamma}^0 = \overline{\Gamma'}^0$.

En particulier, si le groupe algébrique linéaire G sur $\mathbf{R}$ est connexe et n'a aucun quotient anisotrope non nul, (ou, ce qui revient au même, si G est connexe et que les éléments

unipotents de $G(\mathbf{R})$ engendrent un sous-groupe ouvert,) alors tout sous groupe arithmétique de $G(\mathbf{R})$ est Zariski dense, un sous-groupe arithmétique donné de $G(\mathbf{R})$ n'est arithmétique que relativement à (au plus) un modèle de G sur $\mathbf{Q}$, et deux sous-groupes arithmétiques ne seront commensurables que si, et seulement si, ils définissent le même modèle (à isomorphisme de modèle près).

1.1.4. Nous utiliserons également la notion de *réseau arithmétique* d'un groupe de Lie réel *semi-simple connexe* G. Cette classe contient les sous-groupes Γ de G commensurable au stabilisateur, dans G, d'un réseau de la représentation adjointe. Montrons qu'un tel sous-groupe Γ définit bien un réseau de G.

Démonstration. — Comme il suffit de montrer qu'un groupe commensurable à Γ est un réseau, on peut remplacer Γ par le stabilisateur d'un réseau de la représentation adjointe. Dans ce cas Γ contient le noyau de représentation adjointe, et il suffit de montrer que l'image de Γ par la représentation adjointe est un réseau de l'image de G. Or l'image de G est un groupe de Lie semi-simple *linéaire* et l'image de Γ est un sous-groupe arithmétique de l'image de G. Il suffit alors d'appliquer le critère de Borel et Harish-Chandra ([**BHC62**]). □

Un élément de G est dit Ad-unipotent si son image par la représentation adjointe est unipotent. On montre comme précédemment, en appliquant le critère de compacité de Borel ([**Bor69**], Théorème 8.4, [**BHC62**]) plutôt que le critère de Borel et Harish-Chandra, que le réseau Γ est cocompact si et seulement si le seul élément Ad-unipotent de Γ est l'élément neutre.

1.1.5. La famille des *réseaux* arithmétiques est celle des sous-groupes qui sont images d'un sous-groupe de type précédent par un morphisme de groupe de Lie *surjectif* et *à noyau compact*. C'est la notion qui intervient dans le théorème d'arithméticité de Margulis ([**Mar91**]). Ce sont bien des réseaux.

1.2. Sous-groupes de congruence. — Rappelons que $\mathbf{A}_f$ désigne la $\mathbf{Q}$-algèbre des adèles aux places finies. Soit G un groupe algébrique sur $\mathbf{Q}$, plongeons $G(\mathbf{Q})$ dans $G(\mathbf{A}_f)$, et munissons $G(\mathbf{A}_f)$ de la topologie localement profinie usuelle.

1.2.1. Suivant J. Milne ([**Mil90**] p.320) nous appellerons *sous-groupes de congruence de* $G(\mathbf{Q})$ les sous-groupes de $G(\mathbf{Q})$ qui l'on obtient en intersectant $G(\mathbf{Q})$ avec un sous-groupe ouvert et compact de $G(\mathbf{A}_f)$. Lorsque G est linéaire, ce sont des sous-groupes arithmétiques, et ce sont exactement les sous-groupes arithmétiques de $G(\mathbf{Q})$ qui sont ouverts dans $G(\mathbf{Q})$ pour la topologie induite par $G(\mathbf{A}_f)$.

Notons $\overline{G(\mathbf{Q})}$ l'adhérence de $G(\mathbf{Q})$ dans $G(\mathbf{A}_f)$. Par définition, un sous-groupe de congruence Γ est dense dans un ouvert de $\overline{G(\mathbf{Q})}$. Or l'adhérence de Γ est un sous-groupe. C'est donc un sous-groupe ouvert ; c'est en particulier un ouvert. Ainsi, les sous-groupes de congruences de $G(\mathbf{Q})$ sont les sous-groupes de $G(\mathbf{Q})$ dont l'adhérence dans $\overline{G(\mathbf{Q})}$ est compacte et ouverte.

1.2.2. Lorsque G est un sous-groupe fermé de $GL(N)$ défini sur $\mathbf{Q}$, on note parfois $G(\mathbf{Z})$ le groupe $G(\mathbf{Q}) \cap GL(N,\mathbf{Z})$. C'est un sous-groupe arithmétique de $G(\mathbf{Q})$ car c'est précisément le stabilisateur du réseau $\mathbf{Z}^N$ dans une représentation fidèle. C'est aussi un sous-groupe de

congruence, car c'est l'intersection de $G(\mathbf{Q})$ avec le sous-groupe compact et ouvert de $G\left(\widehat{\mathbf{Z}}\right)$ induit par $GL\left(N,\widehat{\mathbf{Z}}\right)$.

Alors un sous-groupe Γ de $G(\mathbf{Q})$ contenu dans $G(\mathbf{Z})$ est de congruence si et seulement si on peut distinguer les éléments de Γ, parmi les éléments de $G(\mathbf{Z})$, en n'imposant qu'un nombre fini de relations de congruence sur les coefficients entiers de la matrice qui les représente. De manière équivalente Γ contient, pour un entier M suffisamment divisible et non nul, le noyau du morphisme $G(\mathbf{Z}) \to GL(N,\mathbf{Z}/(M))$ obtenu en réduisant les coefficients modulo (M). En particulier, pour tout M de $\mathbf{N}_{>0}$, le noyau de ce morphisme est un sous-groupe de congruence de $G(\mathbf{Z})$. On l'appelle *sous-groupe de congruence principal* de *niveau* M. L'auteur ne connaît pas de convention répandue pour noter en toute généralité les sous-groupes principaux de congruence.

Contrairement à la notion de sous-groupe de congruence contenu dans $G(\mathbf{Z})$, qui est intrinsèquement définie par la caractérisation topologique précédente, la notion de sous-groupe principal de congruence dépend en général de la représentation de G comme sous-groupe de $GL(N,\mathbf{Z})$.

1.2.3. Plusieurs auteurs ne définissent les sous-groupes de congruence que comme sous-groupes de $G(\mathbf{Z})$, un sous groupe de $G(\mathbf{Q})$ de la forme $G(\mathbf{Z})$ ayant étant fixé comme précédemment. Mis à part le fait de fixer $G(\mathbf{Z})$, ce n'est pas plus restrictif. En effet, comme d'après [**Bor69**] 7.13 (1), tout sous-groupe arithmétique de $G(\mathbf{Q})$ stabilise un réseau (dans n'importe quelle représentation), les sous-groupes arithmétiques maximaux (dans $G(\mathbf{Q})$) sont de la forme $G(\mathbf{Z})$. Ainsi tout sous-groupe de congruence peut être défini, dans une représentation convenable, à partir de relations comme ci-dessus.

1.2.4. Lorsque G est linéaire, nous dirons qu'un sous-groupe Γ' d'un sous-groupe arithmétique Γ de $G(\mathbf{Q})$ est *relativement de congruence (dans* Γ*)* si ce sous-groupe peut s'obtenir en intersectant Γ avec un sous-groupe de congruence de $G(\mathbf{Q})$, autrement dit si Γ' est ouvert dans Γ pour la topologie induite par $G(\mathbf{A}_f)$. Ce sont les sous-groupes qu'A. Borel, dans [**Bor69**] 7.11, appelle de congruence.

En général les sous-groupes arithmétiques de $G(\mathbf{Q})$ ne sont pas tous de congruence. D'après la caractérisation topologique, un sous-groupe relativement de congruence d'un sous-groupe arithmétique Γ de $G(\mathbf{Q})$ ne sera un sous-groupe de congruence de $G(\mathbf{Q})$ que si Γ lui-même est un sous-groupe de congruence de $G(\mathbf{Q})$.

1.2.5. Contrairement à la notion de sous-groupe arithmétique, la notion de sous-groupe de congruence, n'est pas compatible qux isogénies. Bien que stable par image inverse par une isogénie, elle n'est en général pas stable par image directe.

Détaillons ceci. — Soit $\phi : G \to G'$ est une isogénie définie sur $\mathbf{Q}$ entre deux groupes algébriques sur $\mathbf{Q}$, et notons π son noyau. Notons $\overline{G(\mathbf{Q})}$ (resp. $\overline{G'(\mathbf{Q})}$) l'adhérence de $G(\mathbf{Q})$ dans $G(\mathbf{A}_f)$ (resp. celle de $G'(\mathbf{Q})$ dans $G'(\mathbf{A}_f)$). Le noyau $\ker\overline{\phi_{\mathbf{Q}}}$ de l'application $\overline{\phi_{\mathbf{Q}}} : \overline{G(\mathbf{Q})} \to \overline{G'(\mathbf{Q})}$ est l'intersection de $\pi(\mathbf{A}_f)$ avec $\overline{G(\mathbf{Q})}$. Comme $\pi(\mathbf{A}_f)$ est compact (car π est fini, donc projectif) et $\overline{G(\mathbf{Q})}$ est fermé dans $G(\mathbf{A}_f)$, ce noyau est compact.

Soit Γ' un sous-groupe de congruence de $G'(\mathbf{Q})$: son adhérence $\overline{\Gamma'}$ dans $\overline{G'(\mathbf{Q})}$ est compacte et ouverte. Comme $\overline{\phi_{\mathbf{Q}}}$ est propre et continue, l'image réciproque $\overline{\phi_{\mathbf{Q}}}^{-1}\left(\overline{\Gamma'}\right)$ de $\overline{\Gamma'}$ est un

sous-groupe compact et ouvert. Ainsi l'image réciproque de Γ' par $\phi_{\mathbf{Q}} : G(\mathbf{Q}) \to G'(\mathbf{Q})$, qui est formée des éléments de $\overline{\phi_{\mathbf{Q}}}^{-1}\left(\overline{\Gamma'}\right)$ contenu dans $G(\mathbf{Q})$, c'est-à-dire de l'intersection $\overline{\phi_{\mathbf{Q}}}^{-1}\left(\overline{\Gamma'}\right) \cap G(\mathbf{Q})$, est un sous-groupe de congruence de $G(\mathbf{Q})$.

Les sous-groupes de congruence de $G(\mathbf{Q})$ que l'on obtient ainsi sont les sous-groupes Γ de $G(\mathbf{Q})$ dont l'adhérence $\overline{\Gamma}$, qui et compacte et ouverte dans $\overline{G(\mathbf{Q})}$, contient $\ker\overline{\phi_{\mathbf{Q}}}$.

D'un autre côté, si Γ' est l'image dans $G'(\mathbf{Q})$ d'un sous-groupe de congruence Γ de $G(\mathbf{Q})$, alors $\overline{\phi}_{\mathbf{Q}}^{-1}\left(\Gamma'\right)$ vaut $\pi(\mathbf{Q})\Gamma$. Ainsi Γ' n'est de congruence dans $G'(\mathbf{Q})$ que si $\overline{\Gamma}\pi(\mathbf{Q})$ contient $\ker\overline{\phi_{\mathbf{Q}}}$.

En particulier, comme les sous-groupes compacts et ouverts de $\overline{G(\mathbf{Q})}$ forment une base de voisinages de l'élément neutre, il n'existe un sous-groupe de congruence de $G(\mathbf{Q})$ dont l'image dans $G(\mathbf{Q})$ n'est pas de congruence que si, et seulement si, $\ker\overline{\phi_{\mathbf{Q}}}$ contient *strictement* $\pi(\mathbf{Q})$.

Une reformulation est la suivante. Identifions le complété de $G'(\mathbf{Q})$
- pour la topologie engendré par les sous-groupes de congruence de $G'(\mathbf{Q})$ à $\overline{G'(\mathbf{Q})}$;
- pour la topologie engendré par les images de sous-groupes de congruence de $G(\mathbf{Q})$ à $\overline{G'(\mathbf{Q})}/\pi(\mathbf{Q})$.

Alors le morphisme naturel $\overline{G(\mathbf{Q})}/\pi(\mathbf{Q}) \to \overline{G'(\mathbf{Q})}$ a pour noyau $\frac{\ker\overline{\phi_{\mathbf{Q}}}}{\pi(\mathbf{Q})}$, soit $\frac{\pi(\mathbf{A}_f)\cap\overline{G(\mathbf{Q})}}{\pi(\mathbf{Q})}$.

1.2.5.1. Exemple ([**Ser95**]*).* — Si G est un groupe algébrique linéaire semi-simple connexe de type non compact sur $\mathbf{Q}$, et si $\tilde{G}$ désigne sont revêtement universel alors, d'après le théorème approximation forte, $\widetilde{G}(\mathbf{Q})$, vu comme sous-groupe de $\widetilde{G}(\mathbf{A}_f)$, est *dense*. Dans ce cas, nous avons $\pi(\mathbf{A}_f) = \ker\overline{\phi_{\mathbf{Q}}}$. Or $\pi(\mathbf{A}_f)$ sera distinct de $\pi(\mathbf{Q})$ dès que π n'est le groupe nul.

1.2.5.2. Exemple ([**Rag81**]*).* — L'image dans $PGL(2,\mathbf{Q})$ du sous-groupe principal de congruence de niveau N de $SL(2,\mathbf{Z})$ n'est pas de congruence dès que N contient deux facteurs premiers impairs distincts.

2. Données de Shimura connexes

Fixons, jusque la fin de cette partie, une *donnée de Shimura connexe*. Nous entendons par là que l'on se donne
- un *groupe algébrique réductif connexe* G sur $\mathbf{Q}$,
- un *espace homogène* X *sous le groupe de Lie réel* $G(\mathbf{R})$ comme en [**Del79**], 2.1.1,
- une *composante connexe* X^+ du $G(\mathbf{R})$-espace homogène X,

et que, suivant P. Deligne, nous supposons vérifiés les axiomes (2.1.1.1) à (2.1.1.3) de [**Del79**]. Dans les énoncés (ref) le groupe algébrique G sera supposé presque simple sur $\mathbf{Q}$.

Indiquons que les éléments de X sont concrètement représentés, dans [**Del79**], par des morphismes algébriques $\mathbf{C}^\times \to G(\mathbf{R})$, et que les axiomes (2.1.1.1) à (2.1.1.3) sont inspirés par l'étude des variations de structures de Hodge.

2.1. Structure de G. — Notons Z le centre de G. Le *groupe adjoint* de G, noté G^{ad}, désigne l'image, isomorphe au quotient G/Z, de la représentation adjointe de G. Le *groupe dérivé* $G^{\mathrm{dér}}$ est le *sous-groupe algébrique* de G engendré par les commutateurs (cf. [**Bor91**] I 2.3). Les groupes G^{ad} et $G^{\mathrm{dér}}$ sont semi-simples connexes et reliés par une isogénie ; la composante neutre Z^0 du groupe commutatif Z est un tore algébrique. Le groupe G s'obtient comme une extension centrale de G^{ad} par Z, et est produit presque direct de $G^{\mathrm{dér}}$ et Z^0.

Désignons par $G(\mathbf{R})^+$ (resp. $G^{\mathrm{ad}}(\mathbf{R})^+$, $G^{\mathrm{dér}}(\mathbf{R})^+$, $Z(\mathbf{R})^+$) la composante neutre *du groupe de Lie réel* $G(\mathbf{R})$ (resp. $G^{\mathrm{ad}}(\mathbf{R})$, $G^{\mathrm{dér}}(\mathbf{R})$, $Z(\mathbf{R})$) associé à G (resp. G^{ad}, etc.). Il *ne s'agit en général pas* du sous-groupe qui apparaît dans la conjecture de Kneser-Tits ([**PR94**] 7.2), le sous-groupe engendré par les unipotents rationnels.

D'après (2.1.1.1), (2.1.1.2) et, surtout, (2.1.1.3), le groupe algébrique G^{ad} ou, ce qui revient au même, $G^{\mathrm{dér}}$ est *de type non compact*, au sens où $G^{\mathrm{ad}}(\mathbf{R})$ n'a aucun sous-groupe normal compact connexe *défini sur* $\mathbf{Q}$. De manière équivalente chacun des quasi-facteurs simples du $\mathbf{Q}$-groupe $G^{\mathrm{dér}}$ contient un unipotent non nul défini sur $\mathbf{R}$: chaque quasi-facteur, une fois étendu à $\mathbf{R}$, devient *isotrope* ([**Bor91**], 20.1, 20.6 (ii), 11.1, 11.3 (2), 21.1).

Rappelons quelques propriétés valables pour tout groupe algébrique réel connexe H supposé *linéaire*. Tout d'abord le groupe de Lie réel $H(\mathbf{R})$ associé à H n'est compact que si, et seulement si, H est réductif et anisotrope ; dans ce cas, $H(\mathbf{R})$ n'a qu'une composante connexe ([**Bor91**] V §24.6 (c) (ii), [**PR94**] Théorème 3.1). Plus généralement tout sous-groupe compact de $H(\mathbf{R})$ est le groupe de Lie associé à un sous-groupe algébrique de H. D'après la décomposition de Cartan pour $H(\mathbf{R})$ ([**Mos55**] Théorème 3.2 pour les groupes de Lie ayant un nombre fini de composantes), si K est un sous-groupe compact maximal de $H(\mathbf{R})$, alors $H(\mathbf{R})$ se rétracte sur K ; appliquant π_0 à $H(\mathbf{R})$ et K, il s'ensuit que chaque composante de $H(\mathbf{R})$ rencontre une et une seule composante de K. Notons enfin que $H(\mathbf{R})$ est connexe si H est connexe et simplement connexe ([**PR94**] Proposition 7.6).

2.2. Description de X. — Choisissons comme convention de faire agir le groupe de Lie $G(\mathbf{R})$ *à gauche* sur X : pour h dans X et g dans $G(\mathbf{R})$, nous noterons $g\cdot h$ l'élément de X qui correspond, dans [**Del79**], au morphisme de groupes de Lie réels $z\mapsto g\cdot h(z)\cdot g^{-1}$ de $\mathbf{C}^\times$ dans $G(\mathbf{R})$. Notons que le centre $Z(\mathbf{R})$ de $G(\mathbf{R})$ agit trivialement sur X.

C'est la convention qui correspond, dans le contexte elliptique, à l'action

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : [z:1] \mapsto [a\cdot z+b : c\cdot z+d] = \left[\frac{a\cdot z+b}{c\cdot z+d} : 1\right]$$

par de $SL(2,\mathbf{R})$ homographies sur le demi-plan de Poincaré $\mathfrak{H}$, plongé dans la sphère de Riemann $\mathbf{P}_1(\mathbf{C})$. Cette convention aura pour effet de faire apparaître les réseaux à gauche et les groupes compacts à droite dans les doubles quotients analogues à $SL(2,\mathbf{Z})\backslash SL(2,\mathbf{R})/SO(2,\mathbf{R})$. Afin d'obtenir des quotients analogues dans le contexte adélique, nous introduirons les correspondances de Hecke par une action à droite.

Pour tout élément h de X, notons K_h le stabilisateur de h dans $G(\mathbf{R})$, de sorte que l'application $g\cdot K_h\mapsto g\cdot h$ identifie le quotient $G(\mathbf{R})/K_h$ et X. Il suit de (2.1.1.1) et, surtout, de [**Del79**] 1.2.7 et (2.1.1.2), que K_h est l'image réciproque dans $G(\mathbf{R})$ d'un sous-groupe

compact maximal de $G^{\mathrm{ad}}(\mathbf{R})^+$ (vu comme sous-groupe compact non nécessairement maximal de $G^{\mathrm{ad}}(\mathbf{R})$.) Autrement dit c'est le produit presque direct, dans $G(\mathbf{R})$, de $Z(\mathbf{R})$ par un sous-groupe compact maximal[1] de $G^{\mathrm{dér}}(\mathbf{R})^+$, à savoir $K_h \cap G^{\mathrm{dér}}(\mathbf{R})^+$.

Les orbites de $G(\mathbf{R})^+$ dans X sont connexes et ouvertes ([**PR94**], 3.2 corollaire 2) : ce sont les composantes de X. En particulier $G(\mathbf{R})^+$ stabilise et agit transitivement sur X^+. Il en est donc de même de $Z(\mathbf{R})G(\mathbf{R})^+$ et de $G^{\mathrm{dér}}(\mathbf{R})^+$. Lorsque h appartient à X^+, notons K_h^+ l'intersection de K_h avec $G(\mathbf{R})^+$. Le groupe K_h^+ est connexe. En effet la décomposition de $G(\mathbf{R})^+ = Z(\mathbf{R})^+ \cdot G^{\mathrm{dér}}(\mathbf{R})^+$ induit l'écriture $K_h^+ = Z(\mathbf{R})^+ \cdot \left(K_h \cap G^{\mathrm{dér}}(\mathbf{R})^+\right)$. L'identification de $G(\mathbf{R})/K_h$ avec X induit une identification de $G(\mathbf{R})^+/K_h^+$ à X^+. Par suite X^+ s'identifie à $G^{\mathrm{dér}}(\mathbf{R})^+ / \left(K_h \cap G^{\mathrm{dér}}(\mathbf{R})^+\right)$ ou encore à $G^{\mathrm{ad}}(\mathbf{R})^+ / (K_h/Z(\mathbf{R}))$.

Rappelons que dans $G^{\mathrm{ad}}(\mathbf{R})^+$ les sous-groupes compacts maximaux sont leur propre normalisateur et sont tous conjugués, d'après le théorème de Cartan-Malcev. Il s'ensuit que chaque orbite de $G(\mathbf{R})^+$ dans X s'identifie à l'espace des sous-groupes compacts maximaux de $G^{\mathrm{ad}}(\mathbf{R})^+$, *via* l'application $h \mapsto K_h/Z(\mathbf{R})$. C'est aussi l'espace des *involutions*[2] *de Cartan* sur G^{ad} ou, ce qui revient au même, sur $G^{\mathrm{dér}}$. Ainsi l'espace homogène X^+ est un *espace symétrique de type non compact*. Pour tout point h de X^+, l'involution de Cartan Θ_h : $G^{\mathrm{ad}}(\mathbf{R})^+ \to G^{\mathrm{ad}}(\mathbf{R})^+$ qui fixe $K_h/Z(\mathbf{R})$ induit une involution sur $X^+ = G^{\mathrm{ad}}(\mathbf{R})^+/(K_h/Z(\mathbf{R}))$ admettant h comme unique point fixe.

Le groupe algébrique réel $G^{\mathrm{ad}}_{\mathbf{R}}$ déduit de G^{ad} étant de centre nul (c.-à-d. *adjoint*), il est produit direct, et non seulement presque direct, de ses $\mathbf{R}$-facteurs $\mathbf{R}$-simples. Notons $G^{\mathrm{ad}}_{\mathbf{R}\text{-anis}}$ le sous-groupe produit de ceux de ces facteurs qui sont anisotropes, et $G^{\mathrm{ad}}_{\mathbf{R}\text{-is}}$ le sous-groupe produit de ceux de ces facteurs qui sont isotropes. Le sous-groupe $G^{\mathrm{ad}}_{\mathbf{R}\text{-anis}}(\mathbf{R})$ de $G^{\mathrm{ad}}(\mathbf{R})$ est compact et connexe, et c'est le plus grand sous-groupe normal et compact ; c'est aussi l'intersection des sous-groupes compacts maximaux de $G^{\mathrm{ad}}(\mathbf{R})^+$. La composante neutre $G^{\mathrm{ad}}_{\mathbf{R}\text{-is}}(\mathbf{R})^+$ de $G^{\mathrm{ad}}_{\mathbf{R}\text{-is}}(\mathbf{R})$ est le sous-groupe de $G^{\mathrm{ad}}(\mathbf{R})$ engendré par les éléments unipotents.

Le noyau de l'action de $G(\mathbf{R})$ sur X, le fixateur de X tout entier, est l'image réciproque, dans $G(\mathbf{R})$, de l'intersection, dans $G^{\mathrm{ad}}(\mathbf{R})$ des $K_h/Z(\mathbf{R})$, où h décrit X. C'est donc $G^{\mathrm{ad}}_{\mathbf{R}\text{-anis}}(\mathbf{R})$. Par conséquent, l'image de l'action de $G(\mathbf{R})$ est isomorphe à $G^{\mathrm{ad}}(\mathbf{R})/G^{\mathrm{ad}}_{\mathbf{R}\text{-anis}}(\mathbf{R})$, c'est-à-dire à $G^{\mathrm{ad}}_{\mathbf{R}\text{-is}}(\mathbf{R})$, et l'image de $G(\mathbf{R})^+$ est isomorphe à $G^{\mathrm{ad}}_{\mathbf{R}\text{-is}}(\mathbf{R})^+$.

Le stabilisateur de X^+ dans $G(\mathbf{R})$ contient le sous-groupe $Z(\mathbf{R})G^{\mathrm{dér}}(\mathbf{R})^+$, car ce sous-groupe stabilise X^+. Réciproquement, comme $Z(\mathbf{R})G^{\mathrm{dér}}(\mathbf{R})^+$ agit transitivement sur X^+, tout élément du stabilisateur de X^+, quitte à composer par un élément de $Z(\mathbf{R})G^{\mathrm{dér}}(\mathbf{R})^+$ est contenu dans le fixateur K_h d'un point de X^+. Or $Z(\mathbf{R})G^{\mathrm{dér}}(\mathbf{R})^+$ contient K_h pour tout point h de X. Ainsi le stabilisateur de X^+ dans $G(\mathbf{R})$ est précisément $Z(\mathbf{R})G^{\mathrm{dér}}(\mathbf{R})^+$. Par conséquent l'ensemble des composantes connexes de X est un

[1] Notons que $K_h \cap G^{\mathrm{dér}}(\mathbf{R})$ est le centralisateur de $K_h \cap G^{\mathrm{dér}}(\mathbf{R})^+$ dans $G^{\mathrm{dér}}(\mathbf{R})$; cette intersection contient donc $K_h \cap G^{\mathrm{dér}}(\mathbf{R})^+$ qui est maximal compact dans $G^{\mathrm{dér}}(\mathbf{R})$ et est contenue dans le normalisateur de $K_h \cap G^{\mathrm{dér}}(\mathbf{R})$ dans $G^{\mathrm{dér}}(\mathbf{R})$, ce normalisateur étant maximal compact dans $G^{\mathrm{dér}}(\mathbf{R})$. Il se peut *a priori* $K_h \cap G^{\mathrm{dér}}(\mathbf{R})$ soit strictement entre ces deux groupes.

[2] Suivant en cela la *Théorie des ensemble* de N. Bourbaki, Chapitre II p.17, nous appelons « involution » une permutation qui est sa propre réciproque. En particulier nous considérerons que l'identité *est* une involution, contrairement à [**Hel78**] IV §3 (et l'*Algèbre*, chapitre VI, exercice 32, p. 42.)

torseur sous $G(\mathbf{R})/(Z(\mathbf{R})G^{\text{dér}}(\mathbf{R})^+)$. Ce dernier est un groupe abélien fini isomorphe à l'image de $\pi_0(G^{\text{dér}}(\mathbf{R}))$ dans $\pi_0(G^{\text{ad}}(\mathbf{R}))$.

Terminons cette section en indiquant que les sous-groupes compacts maximaux de $G^{\text{ad}}(\mathbf{R})^+$ s'obtiennent comme produits d'un sous-groupe compact maximal pour chaque facteur de $G^{\text{ad}}(\mathbf{R})^+$. Il suit une décomposition de X^+ en produit des espaces symétriques associés à chacun des facteurs.

Les facteurs simples de $G^{\text{ad}}_{\mathbf{R}}$ sont se rangent en deux catégories, selon

Type III de [**Hel78**] VIII Th. 5.4 : qu'ils sont absolument simples : il proviennent chacun d'un facteur de $G^{\text{ad}}(\mathbf{C})$;

Type IV de [**Hel78**] VIII Th. 5.4 : qu'ils ne sont pas absolument simples : ils proviennent d'une paire de facteurs de $G(\mathbf{C})$ échangés par conjugaison complexe.

Dans le second cas, le facteur en question s'obtient par restriction des scalaires à la Weil à partir d'un groupe simple adjoint G' sur $\mathbf{C}$: ce facteur a pour groupe de points réels $G'(\mathbf{C})$. Comme un tel facteur n'est jamais compact, les facteurs anisotropes de $G^{\text{ad}}_{\mathbf{R}}$ sont tous absolument simples.

Montrons que, sous la condition (2.1.1.2) de [**Del79**], les facteurs isotropes de $G^{\text{ad}}_{\mathbf{R}}$ eux aussi sont absolument simples, autrement dit que, le type IV ci-dessus n'intervient jamais (cf. [**Del79**], 2.3.4).

Démonstration. — Tout sous-groupe compact maximal de $G'(\mathbf{C})$ provient d'une forme réelle compacte de $G'(\mathbf{C})$. Un tel sous-groupe est donc Zariski-dense pour la structure complexe de $G'(\mathbf{C})$. Son centralisateur dans $G'(\mathbf{C})$ est donc le centre de $G'(\mathbf{C})$. Mais G' étant adjoint, ce centre est nul. Ainsi l'involution de Cartan fixant cette forme réelle compacte n'est pas un automorphisme intérieur de $G'(\mathbf{C})$. On peut aussi remarquer cette l'involution de Cartan est la conjugaison complexe relative à la forme réelle, qui n'est pas un automorphisme de G'.

Or d'après (2.1.1.2), les involutions de Cartan de $G^{\text{ad}}(\mathbf{R})^+$ sont des automorphismes intérieurs de $G^{\text{ad}}(\mathbf{R})$. Comme tout sous-groupe compact maximal de $G^{\text{ad}}(\mathbf{R})^+$ s'obtient comme produit d'un sous-groupe compact maximal pour chaque facteur de $G^{\text{ad}}(\mathbf{R})^+$, les involutions de Cartan de $G^{\text{ad}}(\mathbf{R})$ s'écrivent comme produit d'une involution de Cartan sur chaque facteur. Par conséquent les involutions de Cartan, pour chaque facteur de $G^{\text{ad}}(\mathbf{R})^+$, sont des automorphismes intérieurs du groupe réel du facteur correspondant de $G^{\text{ad}}_{\mathbf{R}}$.

Finalement aucun facteur de $G^{\text{ad}}(\mathbf{R})^+$ (isotrope ou non) ne peut être de la forme $G'(\mathbf{C})$. □

2.3. Structure kählérienne. — D'après [**Hel78**] VIII Proposition 4.2, les structures presque complexes invariantes sur X^+ sont intégrables, et par conséquent complexes ([**Hel78**] VIII Théorème 1.2). D'après [**Hel78**] VIII Théorème 7.1, l'espace X^+, muni d'une telle structure, est isomorphe à un domaine complexe borné, et est kählérien ([**Hel78**] VIII Proposition 4.1) pour toute métrique riemannienne invariante (cf. [**Hel78**] VIII Théorème 4.5), et en particulier la métrique de Killing, qui est aussi la métrique de Bergmann ([**Hel78**] VIII Exercice B.1).

On dit que X^+ muni de sa structure complexe et de sa métrique hermitienne invariantes est un *domaine hermitien symétrique*. La donnée de la métrique est parfois sous-entendue, comme dans [**Del79**].

D'après (2.1.1.1) et (2.1.1.2), X est naturellement muni d'une structure complexe invariante. C'est l'unique structure telle que dans [**Del79**], 2.1.1 et 1.1.14 ; elle est donnée explicitement dans [**Mil90**] II.1 p.320 (voir aussi [**Del**]). Ainsi les composantes de X, qui sont en nombre fini et permutées transitivement par $G(\mathbf{R})$, sont toutes isomorphes à un même domaine hermitien symétrique (pour une métrique invariante). D'après [**Del79**] 1.1.17, tous les domaines hermitiens symétriques s'obtiennent de cette manière (pour au moins un choix de métrique invariante).

Pour tout point h de X^+, soit T_hX^+ l'espace tangent à X^+ en h. Une structure presque complexe invariante sur X^+ revient au choix, pour un point h de X^+, d'une structure complexe K_h-invariante sur T_hX^+, c'est-à-dire telle que l'action tangente de K_h commute à l'action de $\mathbf{C}^\times$ par homothéties. Notons $K_{h,\mathbf{R}\text{-is}}$ l'image de K_h dans $G^{\mathrm{ad}}_{\mathbf{R}\text{-is}}(\mathbf{R})^+$, qui agit fidèlement sur X^+. Une telle structure presque complexe induit une représentation continue du groupe $U(1)$ du cercle unité complexe sur T_hX^+. D'après [**Hel78**] VIII Théorème 4.5, cette représentation factorise par l'action du centre de $K_{h,\mathbf{R}\text{-is}}$.

Rappelons que l'involution de Cartan Θ_h agit sur T_hX^+ par $-\mathrm{Id}$, et que comme Θ_h commute à $G^{\mathrm{ad}}_{\mathbf{R}\text{-anis}}(\mathbf{R})$, Θ_h est contenu dans $G^{\mathrm{ad}}_{\mathbf{R}\text{-is}}(\mathbf{R})$. L'action de $U(1)$ définit un sous-groupe à un paramètre de $G^{\mathrm{ad}}_{\mathbf{R}\text{-is}}(\mathbf{R})$ passant par Θ_h, car l'élément -1 de $U(1)$ agit par $-\mathrm{Id}$. Les involutions de Cartan de $G^{\mathrm{ad}}_{\mathbf{R}\text{-is}}(\mathbf{R})$ sont donc contenues dans la composante neutre $G^{\mathrm{ad}}_{\mathbf{R}\text{-is}}(\mathbf{R})^+$. En outre la structure complexe est déterminée par l'action du complexe i, qui agit par un élément de division par 2 de Θ_h dans le centre de $K_{h,\mathbf{R}\text{-is}}$.

Réciproquement tout élément du centre de $K_{h,\mathbf{R}\text{-is}}$ dont le carré est Θ_h, c.-à-d. agit sur T_hX^+ par $-\mathrm{Id}$, définit une structure presque complexe invariante sur X^+ (cf [**Hel78**] VIII Théorème 6.1). On l'a vu, un tel élément, et l'involution de Cartan de K_h, sont nécessairement contenus dans l'image d'un sous-groupe (compact) à un paramètre du centre de K_h.

Nous avons vu que l'existence d'un tel élément, et par suite d'une structure kählerienne invariante sur X, nécessite que les facteurs simples de $G^{\mathrm{ad}}_{\mathbf{R}}$ soient absolument simples. Une condition nécessaire et suffisante est que ces facteurs, munis de leur structure réelle, fassent partie de la liste reproduite en [**Hel78**], X §6.3 (voir aussi [**Del79**] 1.2 et 1.3.9).

Notons que, d'après [**Del79**] Proposition 1.2.7, si $G^{\mathrm{ad}}_{\mathbf{R}\text{-is}}$ est un groupe simple de cette liste, alors le goupe $\pi_0(G^{\mathrm{ad}}_{\mathbf{R}\text{-is}}(\mathbf{R}))$ contient un ou deux éléments, selon le type de $G^{\mathrm{ad}}_{\mathbf{R}\text{-is}}$ (cf. [**Del79**], Corollaire 1.2.8 (i') et (ii')). Écrivons $G^{\mathrm{ad}}_{\mathbf{R}\text{-is}}(\mathbf{R})$, qui est adjoint, en produit direct de ses facteurs simples ; il correspond une écriture de $\pi_0(G^{\mathrm{ad}}_{\mathbf{R}\text{-is}}(\mathbf{R}))$ comme $\mathbf{F}_2$-espace vectoriel dont une base est paramétrée par un l'ensemble des facteurs de $G^{\mathrm{ad}}_{\mathbf{R}\text{-is}}$ ayant deux composantes topologiques. Il s'ensuit une majoration de l'image de $\pi_0(G^{\mathrm{dér}}(\mathbf{R}))$ dans $\pi_0(G^{\mathrm{ad}}(\mathbf{R}))$, et par suite, du nombre de composantes de X.

3. Variétés de Shimura complexes

3.1. Notations. — Notons $\mathbf{A}_f$ la $\mathbf{Q}$-algèbre $\mathbf{Q}\otimes\hat{\mathbf{Z}}$ des *adèles restreintes aux places finies*, ou *adèles finies* sur $\mathbf{Q}$. Nous noterons $G\left(\mathbf{A}_f\right)$ le *groupe topologique* localement compact et totalement discontinu formé des des points de G à coordonnées dans les adèles finies sur $\mathbf{Q}$. Les injections de $\mathbf{Q}$ dans $\mathbf{R}$ et dans $\mathbf{A}_f$ induisent des morphismes injectifs du groupe $G(\mathbf{Q})$ vers $G(\mathbf{R})$ et vers $G(\mathbf{A}_f)$.

Notons $G(\mathbf{Q})^+$ l'intersection de $G(\mathbf{Q})$, vu dans $G(\mathbf{R})$, avec $G(\mathbf{R})^+$ et notons $\overline{G(\mathbf{Q})^+}$ (resp. $\overline{Z(\mathbf{Q})}$) l'adhérence de $G(\mathbf{Q})^+$ (resp. $Z(\mathbf{Q})$), vu cette fois dans $G(\mathbf{A}_f)$. Les sous-groupes fermés $\overline{G(\mathbf{Q})^+}$ et $\overline{Z(\mathbf{Q})}$ de $G(\mathbf{A}_f)$ sont distingués. En effet $\overline{Z(\mathbf{Q})}$ est contenu dans le centre, et $\overline{G(\mathbf{Q})^+}$ contient le groupe dérivé (c'est une conséquence du théorème d'approximation forte).

3.2. Variétés de Shimura de niveau infini. — En [**Del79**] 2.1.4., P. Deligne associe à la donnée de G et X un schéma $M_{\mathbf{C}}(G,X)$ sur $\mathbf{C}$. L'ensemble de ses points complexes est donné ([**Del79**], Proposition 2.1.10) par

$$M_{\mathbf{C}}(G,X)(\mathbf{C}) = G(\mathbf{Q}) \backslash X \times \frac{G\left(\mathbf{A}_f\right)}{\overline{Z(\mathbf{Q})}} . \tag{1}$$

Pour former le quotient précédent, nous faisons agir le groupe $G(\mathbf{Q})$ à gauche et en même temps sur chacun des facteurs : sur X *via* le plongement de $G(\mathbf{Q})$ dans $G(\mathbf{R})$, et par translations sur le groupe quotient $\frac{G(\mathbf{A}_f)}{\overline{Z(\mathbf{Q})}}$ *via* le plongement de $G(\mathbf{Q})$ dans $G(\mathbf{A}_f)$.

3.3. Action de Hecke et Orbites de Hecke. — Considérons l'action à droite, par translations, de $G(\mathbf{A}_f)$ sur le second facteur de $X \times \frac{G(\mathbf{A}_f)}{\overline{Z(\mathbf{Q})}}$. Cette action définit, après passage au quotient, une action à droite du groupe $G(\mathbf{A}_f)$ sur $M_{\mathbf{C}}(G,X)(\mathbf{C})$. Si l'on note les éléments de $\frac{G(\mathbf{A}_f)}{\overline{Z(\mathbf{Q})}}$ comme classes à gauche du sous-groupe distingué $\overline{Z(\mathbf{Q})}$, cette action s'écrit explicitement, pour h dans X, et pour a et g dans $G(\mathbf{A}_f)$,

$$G(\mathbf{Q})\left(h, \overline{Z(\mathbf{Q})} \cdot a\right) \cdot g = G(\mathbf{Q})\left(h, \overline{Z(\mathbf{Q})} \cdot a \cdot g\right). \tag{2}$$

Nous appelerons *orbite de Hecke* une orbite à droite de $G(\mathbf{A}_f)$ dans $M_{\mathbf{C}}(G,X)(\mathbf{C})$.

L'action de $G\left(\mathbf{A}_f\right)$ sur $M_{\mathbf{C}}(G,X)(\mathbf{C})$ provient d'une action de $G\left(\mathbf{A}_f\right)$ sur le *schéma* $M_{\mathbf{C}}(G,X)$ (cf.[**Del79**] (2.1.13.1)). Mentionnons que c'est une *action continue* (cf.[**Gro66**] IV, §8, Proposition 8.2.9, [**Bou71**], Chapitre III, §7.1).

3.4. Ensemble de composantes. — Notons $\pi_0 M_{\mathbf{C}}(G,X)$ l'ensemble des composantes connexes de $M_{\mathbf{C}}(G,X)$, muni de la topologie quotient (cf.[**Del79**] 0.3). Alors $G(\mathbf{A}_f)$ agit continûment sur $\pi_0 M_{\mathbf{C}}(G,X)$.

Il suit de [**Del79**] 2.1.14 que les sous-groupes distingués $\overline{G(\mathbf{Q})^+}$ et $\overline{Z(\mathbf{Q})}$ de $G(\mathbf{A}_f)$ agissent trivialement sur $\pi_0 M_{\mathbf{C}}(G,X)$ et que $\pi_0 M_{\mathbf{C}}(G,X)$ est un torseur sous l'action du groupe abélien quotient $\frac{G(\mathbf{A}_f)}{\overline{G(\mathbf{Q})^+ \cdot Z(\mathbf{Q})}}$. En particulier les composantes de $M_{\mathbf{C}}(G,X)$ ont toutes le même stabilisateur dans $G(\mathbf{A}_f)$, savoir $\overline{G(\mathbf{Q})^+} \cdot \overline{Z(\mathbf{Q})}$. C'est même un torseur topologique[(3)].

En particulier le schéma $M_{\mathbf{C}}(G,X)$ est connexe si et seulement si G satisfait au théorème d'approximation forte ([**PR94**], Théorème 7.12), relativement à la place archimédienne. Autrement dit si G a l'*absolute strong approximation property* au sens de [**PR94**] 7.1.

[(3)] Remarquer que cette action est continue, que $\pi_0 M_{\mathbf{C}}(G,X)$ est séparé car totalement discontinu, et appliquer [**Mil90**], Lemme 10.1.

Comme par hypothèse $G^{\text{dér}}$ est de type non compact, la condition (2) de [**PR94**], Théorème 7.12 est vérifiée : dans notre contexte, l'*absolute strong approximation property* revient à la *semi-simplicité* et la *simple connexité* de G. À noter que dans ce cas, le groupe de Lie $G(\mathbf{R})$ et l'espace X sont connexes, car la proposition 7.6 de [**PR94**] s'applique.

Réciproquement, si G, qui est réductif, n'est pas semi-simple ou n'est pas simplement connexe, alors, d'après [**PR94**] Proposition 7.13, $\pi_0 M_{\mathbf{C}}(G,X)$ est infini. En particulier $M_{\mathbf{C}}(G,X)$ n'est pas de type fini.

Plus généralement le schéma $M_{\mathbf{C}}(G,X)$ n'est pas de type fini si G est non trivial. En particulier il ne s'agit pas d'une variété algébrique. Par exemple, si l'on prend pour G groupe réductif $SL(2)$, et pour domaine connexe X^+ le demi-plan de Poincaré, $M_{\mathbf{C}}(G,X)$ est un schéma affine ayant pour algèbre de fonction régulières les *fonctions modulaires holomorphes* sur X^+ et *méromorphes à l'infini* ([**Mum83**], p. 95) et de niveau indéterminé et arbitrairement grand. Or le niveau des fonctions contenues dans une sous-algèbre de type fini donné sera toujours borné.

3.5. Variétés de Shimura connexes de niveau infini. — Notons $\overline{Z(\mathbf{Q})^+}$ l'intersection de $\overline{G(\mathbf{Q})^+}$ et $\overline{Z(\mathbf{Q})}$. À partir du choix de X^+, parmi les composantes de X, P. Deligne définit un sous-schéma $M^0_{\mathbf{C}}(G,X)$ de $M_{\mathbf{C}}(G,X)$, la *composante neutre de* $M_{\mathbf{C}}(G,X)$ ([**Del79**], définition 2.1.5), dont l'ensemble des points complexes est donné par

$$M^0_{\mathbf{C}}(G,X)(\mathbf{C}) = G(\mathbf{Q})^+ \backslash X^+ \times \frac{\overline{G(\mathbf{Q})^+}}{\overline{Z(\mathbf{Q})^+}}\,, \tag{3}$$

Bien que la notation $M^0_{\mathbf{C}}(G,X)$ ne le fasse pas apparaître, la définition de $M^0_{\mathbf{C}}(G,X)$ dépend toujours du choix de la composante X^+ de X.

Le plongement $\overline{G(\mathbf{Q})^+} \to G(\mathbf{A}_f)$ définit, par passage au quotient, un plongement $M^0_{\mathbf{C}}(G,X)(\mathbf{C}) \to M_{\mathbf{C}}(G,X)(\mathbf{C})$. En effet le stabilisateur de $\overline{G(\mathbf{Q})^+}$ dans $G(\mathbf{Q})\overline{Z(\mathbf{Q})}$ est $G(\mathbf{Q})^+\overline{Z(\mathbf{Q})^+}$.

L'action à gauche de $G(\mathbf{Q})$ sur $X \times \frac{G(\mathbf{A}_f)}{\overline{Z(\mathbf{Q})}}$ se factorise *via* le groupe quotient $G(\mathbf{Q})/Z(\mathbf{Q})$, et ce dernier, muni de la topologie discontinue, agit proprement. On munit ainsi le quotient (1) d'une topologie séparée localement compacte. La topologie que l'on construit de manière analogue sur le quotient (3) est aussi la topologie induite par le plongement $M^0_{\mathbf{C}}(G,X)(\mathbf{C}) \to M_{\mathbf{C}}(G,X)(\mathbf{C})$. Pour ces topologies, $M^0_{\mathbf{C}}(G,X)(\mathbf{C})$ s'identifie à une composante connexe de $M_{\mathbf{C}}(G,X)(\mathbf{C})$.

Notons que, bien que connexe, $M^0_{\mathbf{C}}(G,X)(\mathbf{C})$ n'est en général pas localement connexe, à moins bien sûr, lorsque G est un tore, d'être réduit à un point.

Le plongement $M^0_{\mathbf{C}}(G,X)(\mathbf{C}) \to M_{\mathbf{C}}(G,X)(\mathbf{C})$ provient en fait d'un plongement de schémas $M^0_{\mathbf{C}}(G,X) \to M_{\mathbf{C}}(G,X)$, qui identifie $M^0_{\mathbf{C}}(G,X)$ à une composante géométrique de $M_{\mathbf{C}}(G,X)$. Cette composante permet de distinguer un point du $\frac{G(\mathbf{A}_f)}{\overline{G(\mathbf{Q})^+\cdot Z(\mathbf{Q})}}$-torseur $\pi_0 M_{\mathbf{C}}(G,X)$.

Nous appelerons *orbite de Hecke dans* $M^0_{\mathbf{C}}(G,X)(\mathbf{C})$ la trace sur $M^0_{\mathbf{C}}(G,X)(\mathbf{C})$ laissée par une orbite de Hecke de $M_{\mathbf{C}}(G,X)(\mathbf{C})$. Comme $G(\mathbf{A}_f)$ agit transitivement sur $\pi_0 M_{\mathbf{C}}(G,X)$, cette trace est toujours non vide. Il s'agit donc d'une orbite de $\overline{G(\mathbf{Q})^+}\cdot\overline{Z(\mathbf{Q})}$, le stabilisateur de $M^0_{\mathbf{C}}(G,X)(\mathbf{C})$ dans $G(\mathbf{A}_f)$. Comme l'action de $\overline{Z(\mathbf{Q})}$ est triviale, il s'agit aussi d'une orbite de $\overline{G(\mathbf{Q})^+}$.

4. Modèles canoniques, Action de Galois et Orbites de Hecke

4.1. Modèle canonique. — Si L est un sous-corps de $\mathbf{C}$, un modèle sur L du schéma $M_{\mathbf{C}}(G,X)$ à groupe d'opérateur $G(\mathbf{A}_f)$ désigne la donnée :

- d'un L-schéma $M_L(G,X)$;
- d'une action à droite de $G(\mathbf{A}_f)$ sur $M_L(G,X)$ par automorphismes définis sur L ;
- d'un isomorphisme de $\mathbf{C}$-schémas commutant à l'action de $G(\mathbf{A}_f)$ entre $M_{\mathbf{C}}(G,X)$ et le $\mathbf{C}$-schéma $M_L(G,X)\otimes_L \mathbf{C}$ déduit de $M_L(G,X)$ par extension des scalaires.

Suivant [**Del71**] 3.1, on dira simplement modèle de $M_{\mathbf{C}}(G,X)$ sur L.

Il existe également une notion de modèle canonique. C'est un modèle de $M_{\mathbf{C}}(G,X)$ sur le corps dual $E(G,X)$ vérifiant une condition supplémentaire ([**Del71**], 3.1, [**Del79**] 2.2.5). Un modèle canonique est nécessairement unique, à unique isomorphisme de modèle près.

4.2. Action de Galois. — Soit $M(G,X)$ un modèle de $M_{\mathbf{C}}(G,X)$ sur un sous-corps E de $\mathbf{C}$, par exemple le modèle canonique sur le corps dual. Par hypothèse, $M(G,X)$ est muni d'une action à droite de $G(\mathbf{A}_f)$. Nous en indiquons quelques conséquences immédiates. L'auteur a appris récemment que le matériel de cette section est également contenu, et étendu, dans la prépublication [**UY**] d'E. Ullmo et A. Yafaev.

En choisissant le modèle $M(G,X)$, on s'est donné un isomorphisme $G(\mathbf{A}_f)$-équivariant $M(G,X)\otimes_E \mathbf{C}\to M_{\mathbf{C}}(G,X)$. L'ensemble $M(G,X)(\mathbf{C})$, qui s'identifie à $M(G,X)\otimes_E \mathbf{C}(\mathbf{C})$, s'identifie donc aussi à $M_{\mathbf{C}}(G,X)(\mathbf{C})$, et ces identifications commutent à l'action de $G(\mathbf{A}_f)$.

Par définition $M(G,X)$ est un E-schéma et l'action à droite de chaque élément de $G(\mathbf{A}_f)$ est un automorphisme de $M_{\mathbf{C}}(G,X)$ défini sur E. Autrement dit : pour toute extension L de $E(G,X)$ contenue dans $\mathbf{C}$, l'action à gauche de $\mathrm{Aut}(\mathbf{C}/L)$ sur $M(G,X)(\mathbf{C})$ commute à l'action à droite de $G(\mathbf{A}_f)$. Cela se traduit par la validité de l'identité

$$\sigma(x\cdot g)=\sigma(x)\cdot g \text{ dans } M(G,X)(\mathbf{C}), \tag{4}$$

pour tout point x de $M(G,X)(\mathbf{C})$, tout élément σ de $\mathrm{Aut}(\mathbf{C}/E(G,X))$, et tout élément g de $G(\mathbf{A}_f)$.

Soit $\mathcal{O}$ une orbite de Hecke dans $M(G,X)(\mathbf{C})$, et soit L une extension de $E(G,X)$ contenue dans $\mathbf{C}$. On dira que *l'orbite de Hecke $\mathcal{O}$ est définie sur L* si l'action que $\mathrm{Aut}(\mathbf{C}/L)$ sur $M(G,X)(\mathbf{C})$ laisse $\mathcal{O}$ globalement stable. Soit x un point de $\mathcal{O}$. L'équation (4) a pour conséquence directe que pour tout g de $G(\mathbf{A}_f)$,

$$\mathrm{Aut}(\mathbf{C}/L)\cdot(x\cdot g)=(\mathrm{Aut}(\mathbf{C}/L)\cdot x)\cdot g. \tag{5}$$

Nous voyons en particulier que pour que l'ensemble des conjugués d'un point de $x\cdot g$ de $\mathcal{O}$ soit contenu dans $\mathcal{O}$ il faut et il suffit qu'il en soit de même pour le point x. Ainsi, pour que $\mathcal{O}$ soit définie sur L il faut et suffit que $\mathcal{O}$ contienne l'orbite $\mathrm{Aut}(\mathbf{C}/L)\cdot x$ pour un seul point x de $\mathcal{O}$.

L'équation 5 signifie que les orbites de $\mathrm{Aut}(\mathbf{C}/L)$ dans $\mathcal{O}$ sont échangées par l'action à droite de $G(\mathbf{A}_f)$. Ainsi la propriété suivante ne dépend pas du point x considéré.

Si $\mathcal{O}$ est une orbite de Hecke définie sur L du modèle $M(G,X)$, nous dirons que *l'action de* $\mathrm{Aut}(\mathbf{C}/L)$ *sur l'orbite $\mathcal{O}$ a la propriété d'image ouverte* si l'orbite $\mathrm{Aut}(\mathbf{C}/L)\cdot x$ de x est aussi l'orbite $x\cdot U$ d'un ouvert U de $G(\mathbf{A}_f)$.

Plus généralement, étant donné un sous-groupe normal N de $G(\mathbf{A}_f)$, nous dirons que *l'action de* $\mathrm{Aut}(\mathbf{C}/L)$ *sur l'orbite* $\mathcal{O}$ *a la propriété d'image ouverte relativement à* N si l'orbite $\mathrm{Aut}(\mathbf{C}/L)\cdot x$ de x contient l'orbite $x\cdot U$ d'un ouvert U de N. Cette propriété ne dépend pas non plus du point x choisi. Pour tout nombre premier p, l'image de $G(\mathbf{Q}_p)$ dans $G(\mathbf{A}_f)$ donne un exemple de sous-groupe normal.

PARTIE II
PROPRIÉTÉS D'ÉQUIDISTRIBUTION

5. Une Propriété de finitude sur les groupes arithmétiques

Les résultats de cette section permettent de montrer qu'une des hypothèses du théorème de [**EO06**], l'hypothèse sur le degré des points considérés, est superflue, pourvu que l'on considère des points deux-à-deux distincts. Les résultats présentés ici sont contenus, avec plusieurs compléments, dans l'article [**Ric09b**]. Nous nous proposons ici de montrer plus directement l'énoncé qui nous concerne, le Corollaire 5.2 ci-dessous.

Rappelons ([**EO06**], *Introduction*) que deux sous-groupes Γ_1 et Γ_2 d'un groupe G sont dit *commensurables* si leur intersection est d'indice fini dans Γ_1 et dans Γ_2, tandis que le *commensurateur* de Γ_1 dans G désigne le sous-groupe des éléments de g tels que Γ_1 et $g\Gamma_1 g^{-1}$ soient commensurables.

Soit G un groupe algébrique linéaire semi-simple connexe de type non compact sur $\mathbf{Q}$, et soient Γ et Γ' deux réseaux arithmétiques commensurables de $G(\mathbf{R})$ relativement à G. Rappelons tout d'abord

1. que le normalisateur N de Γ' dans $G(\mathbf{R})$ est un sous-groupe arithmétique de $G(\mathbf{R})$, contenu dans le commensurateur C de Γ' dans $G(\mathbf{R})$, et commensurable à Γ' (et donc aussi commesurable à Γ) ;
2. que tout sous-groupe arithmétique de $G(\mathbf{R})$ n'est contenu que dans un nombre fini et non nul de sous-groupes arithmétiques maximaux ;
3. que tout groupe arithmétique est de type fini ([**BHC62**], Corollaire au Théorème 1) ;
4. que, pour tout entier k, un groupe de type fini ne contient qu'au plus un nombre fini de sous-groupes d'indice au plus k. En particulier il n'y a qu'un nombre fini de sous-groupes contenant un sous-groupe donné d'indice fini.

Les points 1 et 2 résultent du théorème de densité de Borel [**Bor66**] (voir aussi [**All66**]). Le point 3 peut se déduire de la théorie de la réduction, comme rappelé dans [**Bor69**] 9.10. Le point 4, qui est bien connu, se démontre à partir des considérations suivantes. D'une part, tout sous-groupe H de M d'indice k s'obtient comme stabilisateur, pour l'action de M sur M/H, d'un des k points de M/H. D'autre part si M est engendré par n éléments, il y a au plus $(k!)^n$ morphismes de M dans un groupe de permutation sur k éléments donnés, chaque morphisme étant déterminé par l'image des générateurs.

De ces points résulte l'énoncé suivant.

Proposition 5.1. — *Soit G un groupe algébrique linéaire semi-simple connexe de type non compact sur $\mathbf{Q}$, et soient Γ un réseau arithmétique de $G(\mathbf{R})$ relativement à G. Pour tout entier M, il n'existe au plus qu'un nombre fini de sous-groupes arithmétiques de $G(\mathbf{R})$, relativement à G, contenant un sous-groupe de Γ d'indice au plus M.*

Démonstration. — D'après les points 3 et 4 ci-dessus, Γ ne contient qu'un nombre fini de sous-groupes d'indice au plus M. Il suffit donc de considérer les groupes arithmétiques contenant un sous-groupe $\tilde{\Gamma}$ d'indice au plus M donné de Γ.

D'après 2 tout sous-groupe arithmétique est contenu dans un sous-groupe arithmétique maximal, et d'après 2 les sous-groupes arithmétiques maximaux contenant $\tilde{\Gamma}$ sont en nombre fini. Il suffit donc de considérer les groupes arithmétiques intermédiaire entre $\tilde{\Gamma}$ et un sous-groupe arithmétique maximal fixé contenant $\tilde{\Gamma}$.

D'après 4 il n'y a qu'un nombre fini de tels groupes. □

Corollaire 5.2. — *Soit G un groupe de Lie réel semi-simple connexe de type non compact, et soient Γ et Γ' deux réseaux arithmétiques commensurables de G. Notons C le commensurateur de Γ dans G ou, ce qui revient au même, celui de Γ'.*

Alors les orbites à droite de Γ dans $\Gamma'\backslash G$ qui sont finies sont exactement celles qui rencontrent $\Gamma'\backslash C$ ou, ce qui est encore équivalent, qui sont contenues dans $\Gamma'\backslash C$.

Alors l'application $\deg : \Gamma' c \mapsto \left|\Gamma'\backslash\Gamma' c\Gamma\right|$, *de $\Gamma'\backslash C$ vers $\mathbf{N}$ est propre. Autrement dit, pour toute suite $(x_n\cdot\Gamma)_{n\in\mathbf{N}}$ de Γ-orbites finies et deux à deux distinctes dans $\Gamma'\backslash G$, l'entier $|x_n\cdot\Gamma|$ tend vers l'infini.*

La première conclusion est une conséquence la définition du commensurateur. Démontrons la conclusion suivante.

Démonstration. — Il suffit de montrer que pour toute suite $(c_n)_{n\in\mathbf{N}}$ dans C telle que $\left|\Gamma'\backslash\Gamma' c_n\Gamma\right|$ soit borné par un entier, disons k, l'image de $(c_n)_{n\in\mathbf{N}}$ dans $\Gamma'\backslash C$ est compacte, c'est-à-dire finie. Comme, d'après le point 1, N et Γ sont commensurables, il revient au même de montrer que l'image de $(c_n)_{n\in\mathbf{N}}$ dans $N\backslash C$ est finie.

Remarquons que pour tout entier n, on a

$$\left|\Gamma'\backslash\Gamma' c_n\Gamma\right| = \left|(c_n{}^{-1}\Gamma' c_n)\backslash c_n{}^{-1}\Gamma' c_n\Gamma\right| = \left|((c_n{}^{-1}\Gamma' c_n)\cap\Gamma)\backslash\Gamma\right|.$$

La première égalité provient de la bijection $\Gamma' g \mapsto c_n{}^{-1}\Gamma' g$ de $\Gamma'\backslash G$ vers $c_n{}^{-1}\Gamma' c_n\backslash G$. La seconde égalité découle de ce que $(c_n{}^{-1}\Gamma' c_n)\cap\Gamma$ est le stabilisateur dans Γ de la classe $(c_n{}^{-1}\Gamma' c_n)$.

Par hypothèse, l'entier $\left|\Gamma'\backslash\Gamma' c_n\Gamma\right| = \left|((c_n{}^{-1}\Gamma' c_n)\cap\Gamma)\backslash\Gamma\right|$ est borné par k, lorsque n varie. Autrement dit le groupe arithmétique $(c_n{}^{-1}\Gamma' c_n)$ contient un sous-groupe de Γ d'indice au plus k. Or il n'y a qu'un nombre fini de groupes arithmétiques contenant un sous-groupe de Γ d'indice au plus k. Par conséquent, lorsque n varie, le réseau arithmétique $c_n{}^{-1}\Gamma' c_n$ ne décrit qu'un nombre fini de sous-groupes de G. Autrement dit l'image de $(c_n)_{n\in\mathbf{N}}$ dans $N\backslash C$ est finie. □

6. Équidistribution des points de Hecke

Nous reformulons de manière profinie, puis adélique dans la prochaine section, la propriété d'équidistribution de spoints de Hecke de [**EO06**].

Soit G un groupe de Lie réel semi-simple connexe non trivial, et soit Γ un réseau irréductible de G.

Notons C le commensurateur de Γ et notons $\widehat{\Gamma}$ le complété profini de Γ. Soit $\overline{C}$ le groupe localement profini obtenu en complétant C pour la topologie engendrée par les sous-groupes d'indices finis de Γ. Autrement dit $\widehat{\Gamma}$ définit un sous-groupe ouvert de $\overline{C}$.

Tout sous-groupe Γ' de G commensurable à Γ est contenu dans C, et l'adhérence de Γ' dans $\overline{C}$ s'identifie au complété profini $\widehat{\Gamma}'$ de Γ'. En outre $\widehat{\Gamma}'$ définit un sous-groupe compact

et ouvert de $\overline{C}$ et tout sous-groupe compact et ouvert de $\overline{C}$ s'obtient ainsi. Pour retrouver Γ' partant $\widehat{\Gamma}'$, il suffit de former l'intersection de $\widehat{\Gamma}'$ avec C.

La topologie induite sur C par le plongement diagonal de C dans le produit $G\times\overline{C}$ est la topologie discrète. En effet, le groupe Γ est à la fois ouvert dans C, par continuité de $C\to\overline{C}$, et discret, par continuité de $C\to G$. Par conséquent le groupe C, muni de la topologie discrète, agit proprement discontinûment sur l'espace topologique produit $G\times\overline{C}$. Formons le quotient

$$C\backslash G\times\overline{C}.$$

Le groupe topologique $G\times\overline{C}$ agit à droite, par translations, sur ce quotient.

Soit Γ' un réseau de G commensurable à Γ, et faisons agir à droite sur $C\backslash G\times\overline{C}$ le sous-groupe compact et ouvert $\widehat{\Gamma}'$ de $\overline{C}$. Alors le plongement identique de G dans le premier facteur de $G\times\overline{C}$ définit par passage au quotient une identification

$$\Gamma'\backslash G\to C\backslash G\times\overline{C}/\widehat{\Gamma}'. \tag{6}$$

Ces identifications induisent, par passage à la limite projective, une identification

$$\varprojlim_{\Gamma'}\Gamma'\backslash G\to C\backslash G\times\overline{C}. \tag{7}$$

Toute mesure de probabilité sur $\varprojlim_{\Gamma'}\Gamma'\backslash G$ donne, pour tout Γ', une probabilité sur $\Gamma'\backslash G$, par image directe. De même que dans [**Bou63**] §6, se donner une mesure de probabilité μ sur $\varprojlim_{\Gamma'}\Gamma'\backslash G$ revient à se donner, pour tout Γ', une mesure de probabilité $\mu_{\Gamma'}$ sur $\Gamma'\backslash G$, ces mesures s'envoyant les unes sur les autres le long des morphismes de transition du système projectif. On dira que μ est la mesure limite projective des mesures $\mu_{\Gamma'}$.

En outre, suivant la démonstration de [**Bou63**], §6, Lemme 2 (a), on montre que pour qu'une suite de probabilité $(\mu_n)_{n\in\mathbf{N}}$ ait pour limite μ, il faut et il suffit que, pour tout Γ', les suites de mesures correspondantes $(\mu_{n\Gamma'})_{n\in\mathbf{N}}$ ait pour limite $\mu_{\Gamma'}$.

Par exemple, si l'on choisit, pour tout Γ', pour $\mu_{\Gamma'}$ la mesure de probabilité G invariante à droite, la mesure de probabilité μ sur $C\backslash G\times\overline{C}$ que l'on obtient est invariante à droite sous G. On peut montrer qu'elle est en outre invariante à droite sous $\bar{C}$. On dira que μ est la probabilité homogène sur $C\backslash G\times\overline{C}$.

Théorème 6.1. — *Reprenons les notations introduites dans la présente section.*

Soit U un ouvert compact de $\overline{C}$, et soit μ_U la probabilité profinie sur U. Fixons x dans $C\backslash G\times\overline{C}$ et notons μ_{xU} la probabilité sur $C\backslash G\times\overline{C}$ image directe de μ_U par l'application $g\to x\cdot g$ de U vers $C\backslash G\times\overline{C}$. Pour tout g dans $\overline{C}$, notons μ_{xUg} l'image directe de μ_{xU} par la translation à droite par g.

Alors μ_{xUg} tend vers μ lorsque g tend vers l'infini dans $\overline{C}$.

De manière équivalente, si $(g_n)_{n\in\mathbf{N}}$ est une suite de $\overline{C}$ telle que les mesures μ_{xUg_n} soient deux-à-deux distinctes, et si f est une fonction réelle continue bornée sur $C\backslash G\times\overline{C}$, alors $\mu_{xUg_n}(f)$ tend vers $\mu(f)$ lorsque n tend vers $+\infty$.

Démonstration. — Quitte à faire à agir G sur le premier facteur de $G\times\overline{C}$, nous pouvons supposer que x est le point représenant la classe standard C.

Soit Γ' un réseau de G commensurable à Γ, et soit $\widehat{\Gamma}'$ le sous-groupe compact ouvert de $\overline{C}$ correspondant. Alors l'image directe de μ_{xUg} dans $C\backslash G\times\overline{C}/\widehat{\Gamma}'$ correspond, *via* l'identification (6) avec $\Gamma'\backslash G$, à la mesure de comptage normalisée sur l'ensemble fini $C\backslash C(U\cap C)$ (En effet les deux mesures à comparer sont de masse 1 ; comme $CUg\widehat{\Gamma}' = C(U\cap C)g\widehat{\Gamma}'$, l'on a identité de support, et on conclut par invariance sous l'action transitive de $C\cap U$).

Si g tend vers l'infini dans $\bar{C}$, alors Γ est un réseau arithmétique ([**Mar91**], cf. *Introduction*, Théorème (1)), et le cardinal $\#C\backslash C(U\cap C)$ tend vers l'infini (Prop. 5.2). Par conséquent nous pouvons appliquer le résultat principal de [**EO06**]. Nous en déduisons que l'ensemble $C\backslash C(U\cap C)$ s'équidistribue vers la probabilité G-invariante. Par passage à la limite projective, on conclut. □

Corollaire 6.2. — *Soit K un sous-groupe compact de $G\times\overline{C}$. Notons μ^K (resp. μ_{xUgK} l'image directe de μ (resp. μ_{xUg}) dans*

$$C\backslash G\times\overline{C}/K.$$

Alors μ_{xUgK} tend vers μ^K lorsque g tend vers l'infini dans $\overline{C}$.

Démonstration. — Comme K est compact, l'application quotient $C\backslash G\times\overline{C}\to C\backslash G\times\overline{C}/K$ est propre. Elle définit, par composition, un morphisme borné, donc continu, de l'algèbre de des fonctions continues à support compact sur le but vers celle de la source. Le morphisme d'image directe de mesures, défini par dualité, est donc continu, et commute au passage à la limite. □

7. Cas adélique

Supposons maintenant que G est défini sur $\mathbf{Q}$ et que Γ est un sous-groupe arithmétique de G. Alors le commensurateur de Γ contient $G(\mathbf{Q})$. Notons $\overline{G(\mathbf{Q})}$ l'adhérence de $G(\mathbf{Q})$ dans $G(\mathbf{A}_f)$, et $\widehat{G(\mathbf{Q})}$ celle de $G(\mathbf{Q})$ dans $\overline{C}$. Soit K le noyau de congruence de G, c'est-à dire le noyau de l'application naturelle $\widehat{G(\mathbf{Q})}\to\overline{G(\mathbf{Q})}$. C'est un groupe compact.

Remarquons que sur $G(\mathbf{Q})\backslash G(\mathbf{R})\times\overline{G(\mathbf{Q})}$ est une composante connexe de $G(\mathbf{Q})\backslash G(\mathbf{A})$.

Dans ce cas le Corollaire 6.2 se spécialise ainsi.

Corollaire 7.1. — *Le groupe $G(\mathbf{Q})$ définit un réseau de $(G(\mathbf{R})\times\overline{G(\mathbf{Q})})$. Notons μ la probabilité $G(\mathbf{R})\times\overline{G(\mathbf{Q})}$ invariante sur $G(\mathbf{Q})\backslash(G(\mathbf{R})\times\overline{G(\mathbf{Q})})$.*

Soit U l'image dans $\overline{G(\mathbf{Q})}$ d'un ouvert compact de $\widehat{G(\mathbf{Q})}$, par exemple un ouvert compact de $\overline{G(\mathbf{Q})}$, et soit μ_U sa mesure profinie. Fixons x dans $(G(\mathbf{R})\times\overline{G(\mathbf{Q})})$, et soit μ_{xU} la probabilité sur $G(\mathbf{Q})\backslash(G(\mathbf{R})\times\overline{G(\mathbf{Q})})$ image directe de μ_U par l'application $g\to x\cdot g$ de U vers $C\backslash(G(\mathbf{R})\times\overline{G(\mathbf{Q})})$.

Alors μ_{xUg} tend vers μ lorsque g tend vers l'infini dans $\overline{G(\mathbf{Q})}$.

PARTIE III
RÉPARTITION HYPERBOLIQUE D'ORBITES DE HECKE ET D'ORBITES DE GALOIS

Nous appliquons les énoncés de la partie II aux objets de la partie I. Nous nous fixons une donné de Shimura connexe (G, X, X^+) au sens de la partie I et reprenons les notations correspondantes.

8. Mesures hyperboliques

Munissons X de sa topologie d'ensemble analytique réel, et rappelons que $G(\mathbf{A}_f)$ est muni d'une topologie totalement discontinue. Nous appelerons *topologie analytique* sur $M^0_{\mathbf{C}}(G,X)(\mathbf{C})$ la topologie correspondant à la topologie quotient sur $G(\mathbf{Q})^+\backslash X^+ \times \overline{G(\mathbf{Q})^+}$.

Nous parlerons de *probabilité hyperbolique* pour désigner l'unique mesure de probabilité, borélienne pour la topologie analytique, sur $M^0_{/\mathbf{C}}(G,X)(\mathbf{C})$ qui provient d'une mesure sur X^+ invariante sous l'action de $G(\mathbf{R})^+ \times \overline{G(\mathbf{Q})^+}$.

9. Équidistribution des points de Hecke

La proposition suivante est une reformulation de 7.1 dans le contexte des variétés de Shimura.

Proposition 9.1. — *Considérons une donnée de Shimura connexe (G, X, X^+), ainsi que le schéma $M^0_{\mathbf{C}}$ correspondant et la probabilité hyperbolique μ^0 sur $M^0_{\mathbf{C}}(\mathbf{C})$. On suppose que le groupe G est presque simple sur $\mathbf{Q}$.*

Soit U un sous-groupe compact et ouvert de $G(\mathbf{A}_f)$ et soit x un point de $M^0_{\mathbf{C}}(\mathbf{C})$.

Notons μ_{xU} la probabilité U-invariante sur la U-orbite à droite passant par x. Pour tout élément g de $G(\mathbf{A}_f)$, notons μ_{xUg} la probabilité image directe de μ_{xU} sous l'action à droite de g.

Soit $(g_n)_{n\in\mathbf{N}}$ est une suite sans valeur d'adhérence de $G(\mathbf{A}_f)$ dont les termes sont dans $\overline{G(\mathbf{Q})^+}$. Alors la suite $\left(\mu_{xUg_n}\right)_{n\in\mathbf{N}}$ converge vers la probabilité hyperbolique μ^0.

10. Équidistribution galoisienne

Nous reprenons les notations de la proposition précédente.

Proposition 10.1. — *Soit $M^0(G,X)$ un modèle de $M^0(G,X)$ sur un corps E.*

Soit $\mathcal{O}$ une orbite de Hecke dans S, et soit L une extension de E, contenue dans $\mathbf{C}$, sur laquelle l'orbite de Hecke $\mathcal{O}$ est définie. Supposons que $\mathcal{O}$ a la propriété d'image ouverte relativement à L.

Pour tout point x de $\mathcal{O}$, on note μ_x l'unique mesure de probabilité $\mathcal{G}$-invariante sur $x\cdot\mathcal{G}$.

Soit $(g_n)_{n\in\mathbf{N}}$ une suite sans valeur d'adhérence de $G(\mathbf{A}_f)$ dont les termes sont dans $\overline{\iota_f G(\mathbf{Q})^+}$.

Alors la suite $\left(\mu_{xg_n}\right)_{n\in\mathbf{N}}$ converge vers la probabilité hyperbolique sur $\mu_{M^0_{/\mathbf{C}}(G,X)(\mathbf{C})}$.

Cet énoncé est une conséquence de la Proposition 9.1 et de la section précédente.

11. Espaces de modules de variétés abéliennes

Soit A une variété abélienne complexe. La *structure de Hodge* associée est donnée par
- le groupe d'homologie singulière $H_1(A(\mathbf{C});\mathbf{Z})$ (de la variété analytique $A(\mathbf{C})$ associée) et
- le morphisme $h_A : \mathbf{C}^\times \to GL(H_1(A;\mathbf{R}))$ induit par la structure complexe de l'algèbre de Lie de A et l'identification de cette dernière avec $H_1(A;\mathbf{R})$.

Le groupe de Lie $GL(H_1(A;\mathbf{R}))$ a un modèle algébrique sur $\mathbf{Q}$ privilégié induite par le réseau $H_1(A;\mathbf{Z})$. Le *groupe de Mumford-Tate* M_A de A désigne le sous-groupe algébrique de ce modèle obtenu comme l'enveloppe algébrique de $h_A(\mathbf{C}^\times)$ ([**Mum66**]).

Le groupe défini par $\widehat{T}(A) = H_1(A(\mathbf{C});\widehat{\mathbf{Z}})$ s'identifie au module de Tate profini de A. Nous noterons $\widehat{V}(A)$ le *module de Tate adélique* défini par $\widehat{V}(A) = H_1(A(\mathbf{C});\mathbf{A}_f)$. Le groupe $M_A(\mathbf{Q})$ (resp. $M_A(\mathbf{R})$, $M_A(\mathbf{A}_f)$) agit $\mathbf{Q}$-linéairement (resp. etc.) sur $H_1(A(\mathbf{C});\mathbf{Q})$ (resp. etc.). Notons X_A la classe de $M_A(\mathbf{R})$-conjugaison de h_A, et ${X_A}^+$ la composante connexe contenant h_A. Alors $(M_A, X_A, {X_A}^+)$ définit une donnée de Shimura connexe.

Il résulte de [**Del71**] que le schéma $M_{\mathbf{C}}(M_A, X_A)$ est un espace de module grossier pour la classification des variétés abéliennes complexes B *munies* d'une bijection $\mathbf{A}_f$-linéaire

$$\iota_f : H_1(A(\mathbf{C});\mathbf{A}_f) \to H_1(B(\mathbf{C});\mathbf{A}_f)$$

soumises à la condition qu'il *existe*
- une bijection $\iota_\infty : H_1(A(\mathbf{C});\mathbf{R}) \to H_1(B(\mathbf{C});\mathbf{R})$ induisant un isomorphisme $\mathbf{C}$ linéaire de l'algèbre de Lie de B vers celle de A,
- ainsi qu'un isomorphisme ι' de $H_1(A(\mathbf{C});\mathbf{Q})$ vers $H_1(B(\mathbf{C});\mathbf{Q})$

tels que $\iota' \otimes_{\mathbf{Q}} \mathbf{A}$ s'écrive $(\iota_f, \iota_\infty) \circ g$ avec g dans $G(\mathbf{A})$, les isomorphismes de (B, ι_B) vers $(B', \iota_{B'})$ étant les quasi-isogénies φ de $Hom(B, B') \otimes \mathbf{Q}$ telles que $\widehat{V}(\varphi) \circ \iota_B = \iota_{B'}$.

En outre
- l'action de $M_A(\mathbf{A}_f)$ par composition à droite sur ι_f induit l'action de Hecke sur le schéma $M_{\mathbf{C}}(M_A, X_A)$;
- ce problème de module est naturellement défini sur un corps de nombres complexes E, ce qui correspond à un modèle $M(M_A, X_A)$ de $M_{\mathbf{C}}(M_A, X_A)$ sur lequel l'action de $M_A(\mathbf{A}_f)$ est définie ([**DMOS82**]) ;
- étant donné (B, ι_B), il existe une sous-extension de type fini L de $\mathbf{C}/E$ telle que pour tout automorphisme σ de $\mathbf{C}/L$, l'image dans $M_{\mathbf{C}}(M_A, X_A)(\mathbf{C})$ par σ du point représenté par (B, ι_B) soit représenté par $(B, \rho_B(\sigma) \circ \iota_B)$, où $\rho : \mathrm{Aut}(\mathbf{C}/L)$ est une représentation associée à un modèle de B sur L.

Remarquons que si l'on admet la conjecture de Mumford-Tate, renforcée au sens de l'énoncé « *11.4 ?* » de [**Ser94**], alors dans ce dernier cas, le point associé à (B, ι) vérifie la propriété d'image ouverte relativement à $M_B(\widehat{Z})$. En pariculier, si B est la variété abélienne A, que ι est l'identité, cette conjecture implique la propriété d'image ouverte pour A. Dans ce cas nos résultats impliquent l'énoncé suivant.

Théorème 11.1. — *Les notations sont celles qui précèdent. On suppose la conjecture de Mumford-Tate adélique pour A.*

Soit $(\phi_n : A \to A_n)_{n\in\mathbf{N}}$ une suite d'isogénies telles que $(A, \phi_n \otimes \mathbf{A}_f)$ induise un point de $M^0_{\mathbf{C}}(M_A, X_A)(\mathbf{C})$ et dont les classes modulo à gauche modulo $G(\mathbf{Q})$ sont deux-à-deux distinctes.

Alors l'orbite sous $\mathrm{Aut}(\mathbb{C})\mathbf{C}/L$ *du point représentant* $(A, \phi_n \otimes \mathbf{A}_f)$ *s'équidistribue dans* $M^0_{\mathbf{C}}(M_A, X_A)(\mathbf{C})$ *vers la probabilité hyperbolique.*

Notons que la conjecture est vérifiée dans les cas suivants :

1. A est à multiplication complexe : dans ce cas $M^0_{\mathbf{C}}(M_A, X_A)(\mathbf{C})$ est réduit à un point ;
2. A est une courbe elliptique non CM sur un corps de nombres ([**Ser72**]) ;
3. A est une courbe elliptique d'invariant transcendant (Shimura, cf.[**Ric09b**]) ;
4. A est une surface abélienne non CM à multiplication quaternionique ([**Oht74**]).

Dans les trois derniers cas, $M^0_{\mathbf{C}}(M_A, X_A)(\mathbf{C})$ est une courbe de Shimura. Ces cas épuisent les cas de courbes de Shimura où l'on ne recourt pas aux « modèles étranges ».

En utilisant le lemme de Goursat et la conjecture de Tate (démontrée par Faltings), on peut également montrer que la conjecture est vérifiée pour des variétés abéliennes qui sont des produits des exemples donnés.

Il semble que la conjecture de Tate, en combinaison avec les résultats de la seconde partie de ce mémoire et le théorème de Ratner, suffise à impliquer également des propriétés d'équidistribution vers des sous-ensembles homogènes. Or la conjecture de Tate a été démontrée ([**Fal83**]).

Références

[All66] N. D. Allan – « The problem of the maximality of arithmetic groups », in *Algebraic Groups and Discontinuous Subgroups (Proc. Sympos. Pure Math., Boulder, Colo., 1965)*, Amer. Math. Soc., Providence, R.I., 1966, p. 104–109.

[BHC62] A. Borel & Harish-Chandra – « Arithmetic subgroups of algebraic groups », *Ann. of Math. (2)* **75** (1962), p. 485–535.

[Bor66] A. Borel – « Density and maximality of arithmetic subgroups », *J. Reine Angew. Math.* **224** (1966), p. 78–89.

[Bor69] ———, *Introduction aux groupes arithmétiques*, Publications de l'Institut de Mathématique de l'Université de Strasbourg, XV. Actualités Scientifiques et Industrielles, No. 1341, Hermann, Paris, 1969.

[Bor91] ———, *Linear algebraic groups*, second éd., Graduate Texts in Mathematics, vol. 126, Springer-Verlag, New York, 1991.

[Bou] N. Bourbaki – *Éléments de mathématique. XXVI. Groupes et algèbres de Lie. Chapitre 3.*

[Bou63] ———, *Éléments de mathématique. Fascicule XXIX. Livre VI : Intégration. Chapitre 7 : Mesure de Haar.*, Actualités Scientifiques et Industrielles, No. 1306, Hermann, Paris, 1963.

[Bou71] ———, *Éléments de mathématique. Topologie générale. Chapitres 1 à 4*, Hermann, Paris, 1971.

[COU01] L. Clozel, H. Oh & E. Ullmo – « Hecke operators and equidistribution of Hecke points », *Invent. Math.* **144** (2001), no. 2, p. 327–351.

[Del] P. Deligne – « Espaces hermitiens symétriques », `http://www.jmilne.org/math/Documents/index.html`, p. Notes manuscriptes.

[Del71] P. Deligne – « Travaux de Shimura », in *Séminaire Bourbaki, 23ème année (1970/71), Exp. No. 389*, Springer, Berlin, 1971, p. 123–165. Lecture Notes in Math., Vol. 244.

[Del79] ———, « Variétés de Shimura : interprétation modulaire, et techniques de construction de modèles canoniques », in *Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2*, Proc. Sympos. Pure Math., XXXIII, Amer. Math. Soc., Providence, R.I., 1979, p. 247–289.

[DMOS82] P. DELIGNE, J. S. MILNE, A. OGUS & K.-Y. SHIH – *Hodge cycles, motives, and Shimura varieties*, Lecture Notes in Mathematics, vol. 900, Springer-Verlag, Berlin, 1982.

[EO06] A. ESKIN & H. OH – « Ergodic theoretic proof of equidistribution of Hecke points », *Ergodic Theory Dynam. Systems* **26** (2006), no. 1, p. 163–167.

[Fal83] G. FALTINGS – « Endlichkeitssätze für abelsche Varietäten über Zahlkörpern », *Invent. Math.* **73** (1983), no. 3, p. 349–366.

[Gro66] A. GROTHENDIECK – « Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. III », *Inst. Hautes Études Sci. Publ. Math.* (1966), no. 28, p. 255.

[Hel78] S. HELGASON – *Differential geometry, Lie groups, and symmetric spaces*, Pure and Applied Mathematics, vol. 80, Academic Press Inc. [Harcourt Brace Jovanovich Publishers], New York, 1978.

[Mar91] G. A. MARGULIS – *Discrete subgroups of semisimple Lie groups*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 17, Springer-Verlag, Berlin, 1991.

[Mil90] J. S. MILNE – « Canonical models of (mixed) Shimura varieties and automorphic vector bundles », in *Automorphic forms, Shimura varieties, and L-functions, Vol. I (Ann Arbor, MI, 1988)*, Perspect. Math., vol. 10, Academic Press, Boston, MA, 1990, p. 283–414.

[Mos55] G. D. MOSTOW – « Self-adjoint groups », *Ann. of Math. (2)* **62** (1955), p. 44–55.

[Mum66] D. MUMFORD – « Families of abelian varieties », in *Algebraic Groups and Discontinuous Subgroups (Proc. Sympos. Pure Math., Boulder, Colo., 1965)*, Amer. Math. Soc., Providence, R.I., 1966, p. 347–351.

[Mum83] ———, *Tata lectures on theta. I*, Progress in Mathematics, vol. 28, Birkhäuser Boston Inc., Boston, MA, 1983, With the assistance of C. Musili, M. Nori, E. Previato and M. Stillman.

[Oht74] M. OHTA – « On l-adic representations of Galois groups obtained from certain two-dimensional abelian varieties », *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **21** (1974), p. 299–308.

[Pin05] R. PINK – « A combination of the conjectures of Mordell-Lang and André-Oort », in *Geometric methods in algebra and number theory*, Progr. Math., vol. 235, Birkhäuser Boston, Boston, MA, 2005, p. 251–282.

[PR94] V. PLATONOV & A. RAPINCHUK – *Algebraic groups and number theory*, Pure and Applied Mathematics, vol. 139, Academic Press Inc., Boston, MA, 1994, Translated from the 1991 Russian original by Rachel Rowen.

[Rag81] M. S. RAGHUNATHAN – « Isogenies and congruence subgroups », in *Manifolds and Lie groups (Notre Dame, Ind., 1980)*, Progr. Math., vol. 14, Birkhäuser Boston, Mass., 1981, p. 325–336.

[Ric09a] R. RICHARD – « Répartition galoisienne d'une classe d'isogénie de courbes elliptiques », *C. R. Math. Acad. Sci. Paris* **347** (2009), p. 123–127.

[Ric09b] ———, « Répartition galoisienne d'une classe d'isogénie de courbes elliptiques », *Cette thèse* (2009).

[Rud87] W. RUDIN – *Real and complex analysis*, third éd., McGraw-Hill Book Co., New York, 1987.

[Ser72] J.-P. SERRE – « Propriétés galoisiennes des points d'ordre fini des courbes elliptiques », *Invent. Math.* **15** (1972), no. 4, p. 259–331.

[Ser94] ———, « Propriétés conjecturales des groupes de Galois motiviques et des représentations l-adiques », in *Motives (Seattle, WA, 1991)*, Proc. Sympos. Pure Math., vol. 55, Amer. Math. Soc., Providence, RI, 1994, p. 377–400.

[Ser95] _____, « Groupes de congruence (d'après H. Bass, H. Matsumoto, J. Mennicke, J. Milnor, C. Moore) », in *Séminaire Bourbaki, Vol. 10*, Soc. Math. France, Paris, 1995, p. Exp. No. 330, 275–291.

[UY] E. ULLMO & A. YAFAEV – « Generalised tate, mumford-tate and shafarevich conjectures », `http://www.math.u-psud.fr/~ullmo/Prebublications/MTTS1.pdf`.

RODOLPHE RICHARD, Rodolphe RICHARD, IRMAR, Bâtiment 22-23, université de Rennes 1, Campus de Beaulieu, 35000 Rennes

PARTIE II

NON DIVERGENCE S-ARITHMÉTIQUE

GEOMETRIC RESULT ON REPRESENTATIONS OF REDUCTIVE LIE GROUPS

par

Rodolphe RICHARD & Nimish SHAH

Terminological conventions. — All Lie groups are assumed to be *finite dimensional real Lie groups*. By a connected *reductive subgroup H in a semisimple Lie group G*, we mean a closed and connected subgroup whose Lie algebra $\mathfrak{h}$ is a *reductive subalgebra* in the Lie algebra $\mathfrak{g}$ of G, according to [**Bou60**] §6.6 Déf. 5. Namely we ask for the adjoint action of $\mathfrak{h}$ on $\mathfrak{g}$ to be semisimple. Equivalently,

a) the radical of H do not contains unipotent elements of G (cf. [**Bou60**], §6.5 Th.4) and hence H, having central radical, is reductive;
b) every representation of H induced by a finite dimensional linear representation of G is semisimple (see [**Bou60**] §6.6 Cor. 1 and §6.2 Th. 2);
c) H is globally stable under at least one global Cartan involution of G (see [**Mos55a**] and section 2.1).

1. Main application

In this note we prove the following generalisation of Proposition 4.4 from [**EMS97**]: we allow a "reductive *Lie* subgroup H in G" instead of an real *algebraic* subtorus T in G. The section 5 explain how to weaken some hypotheses on G and H.

Theorem 1. — *Let G be a connected semisimple real Lie group and let H be a connected* reductive subgroup in G *(as defined above). Let $Z_G(H)$ denote the centraliser of H inside G and $Z_G(H)^0$ the connected component of $Z_G(H)$ containing the neutral element.*

Then there exists a closed subset Y of G such that

1. *on the one hand we have*

$$G = Y \cdot Z_G(H)^0,$$

2. *on the other hand, given*
   (i) *a subset* Ω *of* H *with nonempty interior,*
   (ii) *a finite dimensional linear representation* ρ*, from* G *into* $GL(V)$*,*
   (iii) *and a norm* $\|-\|$ *on* V*,*
   there exists a constant $c > 0$ *such that*

$$\forall y \in Y, \forall v \in V, \sup_{\omega\in\Omega} \left\|\rho(y\cdot\omega)(v)\right\| \geq c\cdot\|v\|\,. \tag{1}$$

Roughly Theorem 1 means that one cannot uniformly contract a piece $\Omega\cdot v$ of a H-orbit if one acts with an element y which is "orthogonal" to the centraliser of H. The heuristic is the following: might v itself be contracted by y, the $y\Omega y^{-1}$ part in

$$y\cdot\Omega v = y\Omega y^{-1}\cdot yv \tag{2}$$

would be sufficiently expanded in some direction. For y in $Z_G(H)$, (2) yields $y\cdot\Omega v = \Omega\cdot yv$.
Assuming Ω is bounded, the inequality in (1) cannot hold, with uniform constant, for y in $Z_G(H)$ and v in $V\smallsetminus\{0\}$, provided $\left\|yv\right\|/\|v\|$ can be take arbitrarily small values (equivalently, $\rho(Z_G(H))$ is not compact.) As a result, first condition of Theorem 1 seems essentially optimal, for such an Ω.

Our proof do not apparently follow this heuristic, but stems from the original proof of Proposition 4.4, whereas introducing new ideas. It is based on a general decomposition theorem of Mostow (Theorem 4.1 below), elementary linear algebra of Lie algebras and Cartan decompositions (2.2.3) and the convexity of the exponential function (Proposition 1).

Actually, we will prove Theorem 1 under weaker hypotheses on Ω (condition $(*)$ of Corollary 3.4), for an explicitly defined subset Y (see 2.2), and an effective constant c (see formula (20)). Let us first explain how Theorem 1 can be used to simplify article [**EMS97**].

Article [**EMS97**] gives a criterion for non-divergence of certain translates of algebraic measures in some finite volume locally principal homogeneous spaces. The strategy of [**EMS97**] uses two main ideas. First, to adapt linearisation methods from Margulis and Dani (section 2 and 3) to reduce the problem to a statement of linear algebra (cf. [**EMS97**], formula (24)), and then to establish the latter statement. This statement is Theorem 1 and here we provide a new proof.

As a result this note may be used to shorten article [**EMS97**] in several aspects. First of all our note fulfils the purpose of section 4 of [**EMS97**] and our proof may replace the original proof of Proposition 4.4 (p. 67 to 71). More importantly, one can simplify the proof of the main result of [**EMS97**], namely Theorem 1.1, by using our theorem instead of Proposition 4.4. Our Theorem 1 allows us to reduce the proof of Theorem 1.1 in [**EMS97**] to its two first pages, ignoring the steps in pages 74 to 78. Indeed, we only need to adapt section "Reduction to the case of a semisimple H" of [**EMS97**], page 73 as follows (see also our section A):

– replace T by H and apply Theorem 1 above instead of proposition 4.4;
– conclude that formula 29 is the sought for contradiction. Indeed $\pi(\Theta(J_1)) \cdot z_i = \pi(z_i) \cdot \Theta(J_1)$, because z_i commutes with H. But $\pi(Z_G(H))$ was assumed to be compact and J_1 is also compact. Formula 29 is contradictory if C is chosen big enough so that $\pi(C)$ contains $\pi(Z_G(H)) \cdot \Theta(J_1)$, to which belongs $\pi(z_i) \cdot \Theta(J_1)$.

One striking fact about our proof is that it is very effective in most aspects. In particular, it makes it possible to quantitatively estimate the divergence of translated measures in the context of [**EMS97**]. We hope this aspect will lead to new applications. In a following article, we will use the quantitative generalisation of Dani-Margulis linearisation method, in [**KT07**], to obtain effective and generalised form of Theorem 1.1 in [**EMS97**].

2. Preliminaries

We assume all Lie algebras to be real or complex, and finite dimensional.

Let us first recall some more or less well known facts on Cartan involutions and Cartan decompositions. This is for convenience and because for some of these facts no precise reference was found, namely the criterion c) of our terminological conventions and functoriality properties of the Killing form (2.1.10). In order to prove this criterion c), we use a variant of [**Mos55b**] Theorem 6 in the general context of fully reducible linear Lie group as in [**Mos55a**] Theorem 7.3. This variant, although not stated, actually follows from proofs of [**Mos55a**]. We will by the way make precise the definitions we use, as we do not assume our Lie groups to be *linear*, ie. to admit a finite dimensional faithful representation. Our proof of Theorem 1 will only rely on criterion c) of our terminological conventions (proved in 2.1.16), on construction 2.1.15, and on facts collected in remarks 2.2.3.

2.1. Cartan involutions. — Let $\mathfrak{g}$ be a finite dimensional real Lie algebra and denote its adjoint representation by $\mathrm{ad} : \mathfrak{g} \to \mathfrak{gl}(\mathfrak{g})$. Recall that the *Killing form* on $\mathfrak{g}$ denotes the real bilinear form on $\mathfrak{g} \times \mathfrak{g}$ which sends (X, Y) to $B(X, Y) = \mathbf{Tr}(\mathrm{ad}(X)\mathrm{ad}(Y))$ ([**Bou60**], §3.6 Déf. 4). This form is obviously symmetric, and is nondegenerate if and only if $\mathfrak{g}$ is semisimple ([**Bou60**], §6.1 Th. 1).

2.1.1. If G is a *linear* real Lie group with Lie algebra $\mathfrak{g}$, then isotropic nonzero vectors of B are exactly the generators of (one dimensional and non trivial) Ad-unipotent subgroups; nonzero nonisotropic vectors of positive (resp. negative) norm are exactly the generators of noncompact one parameter subgroups of semisimple elements (resp. one parameter compact subgroup). The Killing form is *completely invariant* ([**Bou60**] III. §6 Prop. 10); equivalently, the image $\exp(\mathrm{ad}(\mathfrak{g}))$ of $\mathrm{ad}(\mathfrak{g})$ in $GL(\mathfrak{g})$ is contained in the orthogonal group of B. In particular, for any X and Y in $\mathfrak{g}$, $\exp(\mathrm{ad}(X))(Y)$ is isotropic (resp. positive, negative) if and only if Y is.

2.1.2. A *Cartan involution* of a real Lie algebra $\mathfrak{g}$ means an involution θ of the algebra $\mathfrak{g}$ such that the bilinear form $(X,Y) \mapsto B_\theta(X,Y) = -B(X,\theta(Y))$ is symmetric and strictly positive definite ([**Hel78**], III §7). In particular B is nondegenerate and $\mathfrak{g}$ is semisimple.

2.1.3. Remark that if a linear subspace $\mathfrak{z}$ of $\mathfrak{g}$ is invariant under θ, then its orhtogonals with respect to B and B_θ coincide. Consequently, as B_θ is anisotropic, $\mathfrak{z}$ and its orthogonal are supplementary. In particular, θ stable subspace are globally self-adjoint for θ.

2.1.4. Consider the adjoint representation $\mathrm{ad} : \mathfrak{g} \to \mathfrak{gl}(\mathfrak{g})$ and a Cartan involution θ on $\mathfrak{g}$. Then the adjunction involution on $\mathfrak{gl}(\mathfrak{g})$ with respect to B_θ is an extension of θ.

Proof. — Let X be in $\mathfrak{g}$, let $\mathrm{ad}_X : Y \mapsto [X,Y]$ be its image in $\mathfrak{gl}(\mathfrak{g})$. We need to show that $\mathrm{ad}_\theta(X)$ is the adjoint of ad_X with respect to B_θ, namely, that for any Y and Z in $\mathfrak{g}$

$$B_\theta(\mathrm{ad}_X(Y), Z) = B_\theta(Y, \mathrm{ad}_{\theta(X)} Z).$$

By definition of ad and B_θ this equality means

$$B([X,Y],\theta(Z)) = B(X,\theta([\theta(X),Z])).$$

But $B([X,Y],\theta(Z)) = B(Y,[X,\theta(Z)])$ follows from invariance ofthe Killing form whereas the identity $\theta([\theta(X),Z]) = [X,\theta(Z)]$ follows from the fact that θ is an algebra involution. □

2.1.5. A *global Cartan involution* of a connected real Lie group G with Lie algebra $\mathfrak{g}$ is an involution $\Theta : G \to G$ whose differential at the neutral element is a Cartan involution of $\mathfrak{g}$. Every Cartan involution of $\mathfrak{g}$ extends to G.

Proof. — We may assume G is semisimple, else there is no Cartan involution. According to [**Bou**] §6.2 Théo. 1, we any Cartan involution θ has an extension $\widetilde{\Theta}$ to the universal cover $\widetilde{G}$ of G. It will be enough to show that $\widetilde{\Theta}$ fixes elementwise the center $Z\big(\widetilde{G}\big)$ of $\widetilde{G}$. As $Z\big(\widetilde{G}\big)$ is a characteristic subgroup, it is stable under automorphisms. Hence $\widetilde{\Theta}$ descend to an involution Θ^{ad} the adjoint group $G^{\mathrm{ad}} = \widetilde{G}/Z\big(\widetilde{G}\big)$, which is linear. It will be enough to show that the induced action of $\widetilde{\Theta}$ on the fundamental group $\pi_1(G^{\mathrm{ad}})$ is trivial. But, from Cartan decomposition ([**Mos55a**], Theorem 3.2), G^{ad} retracts to any of its maximal compact subgroups, and one such a maximal compact subgroup is the fixed locus of Θ^{ad}. □

2.1.6. We will say that a closed subgroup of a *connected semisimple* Lie group G is *projectively compact* if its image under the adjoint representation $\mathrm{Ad} : G \to GL(\mathfrak{g})$ is compact. When G is *linear*, this property is equivalent to compactness. In general this property is stable under direct image by morphisms of semisimple connected Lie groups, and inverse images by isogenies. When G is connected, semisimple

and *linear*, the set of fixed point of a given global Cartan involution defines a maximal compact subgroup (recall that G is connected). If G is only assumed to be connected and semisimple, writing G as a central covering of its adjoint group, we deduce that the set of fixed point of a given global Cartan involution defines a maximal projectively compact subgroup.

2.1.7. A semisimple real Lie algebra is said to be *compact* if its Killing form is totally negative. One actually needs only to ask the Killing form to be *anisotropic*.

2.1.8. Every semisimple Lie algebra $\mathfrak{g}$ is a direct product of its simple ideals ([**Bou60**] §6.2, Cor. 1), and these simple ideals are pairwise orthogonal for the Killing form ([**Bou60**] §6.1, Cor. 1). For any Cartan involution θ of $\mathfrak{g}$, one has $-B(X,\theta(X)) > 0$ whenever $X \neq 0$. Consequently the image $\theta(X)$ of a non zero element X of $\mathfrak{g}$ cannot be orthogonal to X. *A fortiori* θ cannot send any simple ideal of $\mathfrak{g}$ to an orthogonal ideal. Consequently, a Cartan involution of $\mathfrak{g}$ stabilises each simple ideal of $\mathfrak{g}$. As ideals of $\mathfrak{g}$ are sum of simple ideals ([**Bou60**] §6.2, Cor. 1), a Cartan involution of $\mathfrak{g}$ stabilises each ideal of $\mathfrak{g}$.

2.1.9. According to [**Bou60**] §3.7, Prop. 9, the restriction of the Killing form of $\mathfrak{g}$ to an ideal $\mathfrak{a}$ is the Killing form of $\mathfrak{a}$. It follows that the restriction of a Cartan involution to an ideal is a Cartan involution, and that an endomorphism of $\mathfrak{g}$ is a Cartan involution if and only if it stabilises each simple ideal and its restriction to each simple ideal is a Cartan involution. These restrictions being nondegenerate, a simple ideal do not intersect its orthogonal: the orthogonal of a simple ideal, and more generally of any ideal $\mathfrak{a}$, is reduced to the simple ideals not belonging to $\mathfrak{a}$.

2.1.10. Consider a semisimple Lie algebra $\mathfrak{g}$ and a morphism of Lie algebras $\phi : \mathfrak{g} \to \mathfrak{g}'$. Its kernel $\ker(\phi)$ is an ideal whose orthogonal $\ker(\phi)^\perp$ is a supplementary ideal; ϕ sends $\ker(\phi)^\perp$ bijectively onto $\phi(\mathfrak{g})$. In particular $\phi(\mathfrak{g})$ is a semisimple Lie algebra; any Cartan involution of $\mathfrak{g}$ stabilises $\ker(\phi)$; the induced involution on $\phi(\mathfrak{g})$ is a Cartan involution. We will call the latter the *image Cartan involution*.

2.1.11. Given a Cartan involution θ on a semisimple Lie algebra $\mathfrak{g}$, the associated *Cartan decomposition* denotes the decomposition $\mathfrak{g} = \mathfrak{k} \oplus \mathfrak{p}$ of $\mathfrak{g}$ as a direct sum of the eigenspace $\mathfrak{k}$ (resp. $\mathfrak{p}$) of θ associated with the eigenvalue $+1$ (resp.-1). Clearly Cartan involutions and associated Cartan decompositions determine each other. By definition θ is self-adjoint, hence the eigenspaces $\mathfrak{k}$ and $\mathfrak{p}$ are the orthogonal to each other. Consequently, the Cartan involution θ is determined by $\mathfrak{k}$ only (knowing B). Note that $\mathfrak{k}$ is a maximal negative anisotropic subspace of B and a subalgebra of $\mathfrak{g}$ (it satisfies Frobenius integrability condition), and that $\mathfrak{p}$ is maximal positive anisotropic linear subspace and is $\mathfrak{k}$-invariant.

2.1.12. Let denote $\mathfrak{g}_{\mathbf{C}} = \mathfrak{g} \otimes_{\mathbf{R}} \mathbf{C}$ the complexified Lie algebra, obtained from $\mathfrak{g}$ by extending the base field. We may also view $\mathfrak{g}_{\mathbf{C}}$ as a *real* Lie algebra, by Weil restriction of scalars. According to [**Hel78**] III. Prop. 7.4, every *Cartan decomposition*

of $\mathfrak{g}$, as defined in [**Hel78**] p. 183 actually comes from a Cartan involution, as defined above, and these Cartan decompositions are exactly the restriction to $\mathfrak{g}$ of the Cartan decompositions of the real Lie algebra $\mathfrak{g}_{\mathbf{C}}$ which are invariant (factorwise) under complex conjugation. The anisotropic subalgebra of $\mathfrak{g}_{\mathbf{C}}$ corresponding to the latter are the *compact* (see 2.1.7) real forms of the complex Lie algebra $\mathfrak{g}_{\mathbf{C}}$ wich are *invariant* under the complex conjugation relative to the real structure induced by $\mathfrak{g}$ (see also [**Mos55a**], section 2).

2.1.13. For a *reductive* lie algebra $\mathfrak{g}$, *together with* an embedding $\mathfrak{g} \to \mathfrak{gl}(V)$, for some V of finite dimension, a *real form* $\mathfrak{k}$ of $\mathfrak{g}_{\mathbf{C}}$ is said to be *compact* if $\exp(\mathfrak{k})$ is compact in $GL(V \otimes \mathbf{C})$, and *invariant* if $\mathfrak{k}$ is globally invariant under the complex conjugation on $\mathfrak{g}_{\mathbf{C}}$ relative to $\mathfrak{g}$. According to [**Mos55a**], lemma 6.2, there exists such a compact form if and only if the action of $\mathfrak{g}$ on V is semisimple (the "only if" part is known as "Weyl's unitary trick"). In such a case, we will say that $\mathfrak{g}$ together with its embedding is a *linear fully reducible* subalgebra of $\mathfrak{gl}(V)$.

2.1.14. The preceding points implies that invariant compact forms generalises to linear fully reducible Lie algebra the Cartan decompositions of semisimple Lie algebras. By using [**Mos55a**] Theorem 4.1 as in proof of the exponented Theorem 5.1[1] of [**Mos55a**], given a nested sequence of linear fully reducible subalgebras of $\mathfrak{gl}(V)$, one can form a nested sequence of invariant compact real forms of the corresponding complexified linear algebras.

2.1.15. Consider now a finite dimensional linear representation $\rho : \mathfrak{g} \to \mathfrak{gl}(V)$ of a semisimple Lie algebra. Then, given a Cartan involution of $\mathfrak{g}$ we get a Cartan involution of $\rho(\mathfrak{g})$, by 2.1.10. This Cartan involution corresponds to an invariant compact real form on $\rho(\mathfrak{g})_{\mathbf{C}}$, by (2.1.12), which we can extend to $\mathfrak{gl}(V)$, by (2.1.14).

Any such extension is the unitary group of a euclidean structure on V, unique up to proportionality. With respect to this structure $\rho(\mathfrak{g})$ is globally self-adjoint ([**Mos55a**], proof of Theorem 5.1), and such that the euclidean adjunction extend the opposite of the image Cartan involution (2.1.10) on $\rho(\mathfrak{g})$ (*loc. cit.*, formula (2)).

2.1.16. Criterion c) of our terminological conventions clearly follows from the corresponding statement at the level of Lie algebras, which we now prove. Namely *a real subalgebra $\mathfrak{h}$ of a (finite dimensional) real semisimple Lie algebra $\mathfrak{g}$ is globally invariant under some Cartan involution of $\mathfrak{g}$ if and only if the adjoint action of $\mathfrak{h}$ on $\mathfrak{g}$ is fully reduicible.*

Proof. — Consider a subalgebra $\mathfrak{h}$ of a semisimple Lie algebra $\mathfrak{g}$. If $\mathfrak{h}$ is globally invariant under θ, its image under $\mathrm{ad} : \mathfrak{g} \to \mathfrak{gl}(\mathfrak{g})$ is globally self-adjoint for B_θ, according to 2.1.4. As B_θ is *anisotropic*, the orthogonal of a $\mathrm{ad}_{\mathfrak{h}}$-stable subspace defines a stable *supplementary* $\mathrm{ad}_{\mathfrak{h}}$-subspace. It implies that $\mathfrak{h}$ acts fully reducibly on $\mathfrak{g}$.

Assume now that $\mathfrak{h}$ acts fully reducibly on $\mathfrak{g}$. Denote extension of scalars by an subscripts. Then the linear subalgebra $\mathrm{ad}(\mathfrak{h})_{\mathbf{C}}$ of $\mathfrak{gl}(\mathfrak{g})_{\mathbf{C}}$ has an invariant compact real form (2.1.13). This real form is contained in an invariant compact real form of $\mathrm{ad}(\mathfrak{g})_{\mathbf{C}}$ (2.1.14). The latter is associated with a Cartan involution θ of $\mathfrak{g}$ (2.1.12). Applying to $\mathfrak{h}$ the Lie algebra analogue of decomposition (2) in proof of Theorem 5.1 in [**Mos55a**], we see that $\mathfrak{h}$ is invariant under θ, each factor being contained in a factor of the corresponding Cartan decomposition of $\mathfrak{g}$. □

2.2. Notational conventions. — In the next sections we will often consider the following situation. Let us fix, once for all, our notations.

2.2.1. General notations. — Let G be a connected semisimple Lie group, let H be connected reductive Lie subgroup in G (see conventions). Let Θ be a global Cartan involution (cf. 2.1.2, 2.1.5) of G under which H is globally invariant (conventions, criterion c)). We denote by $Z_G(H)$ the centraliser of H in G, and by K the maximal projectively compact subgroup made of fixed elements of Θ (cf. 2.1.6).

Denote by $\mathfrak{g}$, $\mathfrak{h}$, $\mathfrak{z}_{\mathfrak{g}}$, $\mathfrak{k}$ the Lie algebra of G, H, $Z_G(H)$, and K respectively, and denote by θ the differential of Θ at the neutral element.

We write $\mathfrak{k}^{\perp}$ and ${\mathfrak{z}_{\mathfrak{g}}}^{\perp}$ for the orthogonal, with respect to the Killing form (cf. 2.1) on $\mathfrak{g}$, to $\mathfrak{k}$ and $\mathfrak{z}_{\mathfrak{g}}$ respectively. We define $\mathfrak{p} = \mathfrak{k}^{\perp} \cap {\mathfrak{z}_{\mathfrak{g}}}^{\perp}$, $P = \exp(\mathfrak{p})$ and $Y = K \cdot P$. Finally, $B_\theta : \mathfrak{g} \times \mathfrak{g} \to \mathbf{R}$ will be the strictly positive definite symmetric bilinear form on $\mathfrak{g}$ associated with θ (cf. 2.1.2).

2.2.2. Relative notations. — When considering, in situation 2.2.1, a finite dimensional linear representation $\rho : G \to GL(V)$, we shall use the following notations.

We denote by $\mathbf{d}\rho : \mathfrak{g} \to \mathfrak{gl}(V)$ the tangential representation of ρ and by $\mathfrak{z}$ the commutant of $\rho(H)$ in $\mathfrak{gl}(V)$. The Trace map on $\mathfrak{gl}(V)$ is denoted by $\mathbf{Tr} : \mathfrak{gl}(V) \to \mathbf{R}$, and the *trace form* means the bilinear form $(X, Y) \mapsto \mathbf{Tr}(XY)$ on $\mathfrak{gl}(V)$ (it is the *bilinear form associated with the* $\mathfrak{gl}(V)$*-module* V, according to [**Bou60**], III §3.6, Déf. 4.) We write $\mathfrak{z}^{\perp}$ for the orthogonal of $\mathfrak{z}$ for the trace form.

Using 2.1.15, we fix a euclidean structure on V such that the opposite, say $\theta_V : \mathfrak{gl}(V) \to \mathfrak{gl}(V)$, of its euclidean adjunction involution stabilises $\mathbf{d}\rho(\mathfrak{g})$ and extend the image Cartan involution of θ on $\mathbf{d}\rho(\mathfrak{g})$.

2.2.3. Remarks. — In such a situation, our recalls 2.1 on Cartan involutions has the following immediate consequences.

1. In $\mathfrak{g}$, the subspaces $\mathfrak{k}$, $\mathfrak{h}$, and hence $\mathfrak{z}_{\mathfrak{g}}$, are globally invariant under θ.
2. The orthogonals of $\mathfrak{k}$ (resp. $\mathfrak{h}$, $\mathfrak{z}_{\mathfrak{g}}$) in $\mathfrak{g}$ with respect to the Killing form or with respect to B_θ are the same. This orthogonal is supplementary to $\mathfrak{k}$ (resp. $\mathfrak{h}$, $\mathfrak{z}_{\mathfrak{g}}$) in $\mathfrak{g}$.
3. The subspace ${\mathfrak{z}_{\mathfrak{g}}}^{\perp}$ of $\mathfrak{g}$ is invariant under the adjoint action of H; it is the unique supplementary H-stable subspace to the isotypic component $\mathfrak{z}_{\mathfrak{g}}$ in the H-module $\mathfrak{g}$.

4. The map $\mathbf{d}\rho : \mathfrak{g} \to \mathfrak{gl}(V)$ commute with the involutions θ on $\mathfrak{g}$ and θ_V on $\mathfrak{gl}(V)$.
5. The subspace $\mathfrak{z}^\perp$ of $\mathfrak{gl}(V)$ is invariant under the adjoint action of H; it is the unique supplementary H-stable subspace to the isotypic component $\mathfrak{z}$ in the H-module $\mathfrak{gl}(V)$.
6. The map $\mathbf{d}\rho : \mathfrak{g} \to \mathfrak{gl}(V)$ sends $\mathfrak{z}_\mathfrak{g}$ to $\mathfrak{z}$ and ${\mathfrak{z}_\mathfrak{g}}^\perp$ to $\mathfrak{z}^\perp$.
7. In $\mathfrak{gl}(V)$, the subspaces $\mathbf{d}\rho(\mathfrak{k})$, $\mathbf{d}\rho(\mathfrak{z}_\mathfrak{g})$, $\mathbf{d}\rho(\mathfrak{h})$ and hence $\mathfrak{z}$ and $\mathfrak{z}^\perp$, are globally invariant under θ_V.
8. The orthogonal projection $\pi_\mathfrak{z} : \mathfrak{gl}(V) \to \mathfrak{z}$ with respect to the trace form commutes with θ_V; it sends self-adjoint endomorphisms to self-adjoint endomorphisms.
9. The map $\mathbf{d}\rho$ sends elements of $\mathfrak{k}^\perp$ to self-adjoint endomorphisms of V.

Proof. — **1.** By definition of $\mathfrak{k}$, assumption on H, and construction of $\mathfrak{z}_\mathfrak{g}$ from $\mathfrak{h}$. **2.** From 1., definition of B_θ and anisotropy of B_θ (cf. 2.1.3). **3.** Both $\mathfrak{z}_\mathfrak{g}$ and B are invariant under adjoint action of H; the isotypic components are uniquely defined (13, §3.1). **4.** Definition of θ_V. **5.** See 3. **6.** As $\mathbf{d}\rho$ commutes with the adjoint action of H, it preserves isotypic decomposition. **7.** From 1. and 3., from construction of $\mathfrak{z}$ from $\mathbf{d}\rho(\mathfrak{h})$, and from selfadjointness of the euclidean adjunction with respect to the Trace form (it can be checked in an orhtogonal basis). **8.** Both $\mathfrak{z}$ and orthogonality are invariant under θ_V; self-adjoint means fixed by θ_V. **9.** Follows from 4. □

3. Effective statements

Our effective statements will rely on the corollary 3.2 of the following result. Note that the property that p "can only go to infinity in directions orthogonal to $\mathfrak{z}_\mathfrak{g}$" is only used in the next proof, in order to get a uniform lower bound on the eigenvalues.

Theorem 3.1. — *We consider the situation 2.2.1 and 2.2.2.*

For any p in P, the endomorphism $\pi_\mathfrak{z}(\rho(p))$ of V is self-adjoint, positive definite, and has no eigenvalue smaller than 1.

Proof. — Fix p in P and write $p = \exp(\wp)$ for some $\wp$ in $\mathfrak{p}$. From $\mathfrak{p} = \mathfrak{k}^\perp \cap {\mathfrak{z}_\mathfrak{g}}^\perp$ follows that $\mathbf{d}\rho(\wp)$ belongs to both $\mathbf{d}\rho(\mathfrak{k}^\perp)$ and $\mathbf{d}\rho({\mathfrak{z}_\mathfrak{g}}^\perp)$. Consequently $\mathbf{d}\rho(\wp)$ is self-adjoint (remark 9) and orthogonal to $\mathfrak{z}$ with respect to the trace form (remark 6). We will write S for $\mathbf{d}\rho(\wp)$. By [**Bou**] §4. Cor. 2, we get $\rho(p) = \exp(S)$, so that $\rho(p)$ is self-adjoint and definite positive. As a result, $\pi_\mathfrak{z}(\rho(p))$ is self-adjoint (remark 8), and belongs to $\mathfrak{z}$, the image of $\pi_\mathfrak{z}$.

Let λ be an eigenvalue of $\pi_\mathfrak{z}(\rho(p))$, and let π_λ be the corresponding spectral projector. We saw that $\pi_\mathfrak{z}(\rho(p))$ is self-adjoint and commutes with H, and it is well known that π_λ belongs to the subalgebra generated by $\pi_\mathfrak{z}(\rho(p))$. Consequently π_λ is self-adjoint and commutes with H. In particular, π_λ belongs to $\mathfrak{z}$.

The difference $\pi_{\mathfrak{z}}(\rho(p)) - \rho(p)$ belongs to the kernel of the projector $\pi_{\mathfrak{z}}$: it is orthogonal to $\mathfrak{z}$, and, in particular, to π_λ. Consequently,

$$\mathbf{Tr}(\pi_{\mathfrak{z}}(\rho(p))\pi_\lambda) = \mathbf{Tr}(\rho(p)\pi_\lambda) = \mathbf{Tr}(\exp(S)\pi_\lambda).$$

On the other hand, $\mathbf{Tr}(\pi_{\mathfrak{z}}(\rho(p))\pi_\lambda)$ equals $d_\lambda \cdot \lambda$, where d_λ is the rank of π_λ and $d_\lambda > 0$.

From proposition 1, we have the inequality $\mathbf{Tr}(\exp(S)\pi_\lambda) \geq d_\lambda \cdot \exp(\mathbf{Tr}(S\pi_\lambda)/d_\lambda)$. Because π_λ is in $\mathfrak{z}$, and S is orthogonal to $\mathfrak{z}$, $\mathbf{Tr}(S\pi_\lambda) = 0$. As a consequence $\lambda \geq 1$. Indeed

$$d_\lambda \cdot \lambda = \mathbf{Tr}(\pi_{\mathfrak{z}}(\rho(p))\pi_\lambda) = \mathbf{Tr}(\exp(S)\pi_\lambda) \geq d_\lambda \cdot \exp(\mathbf{Tr}(S\pi_\lambda)/d_\lambda) = d_\lambda \cdot 1. \tag{3}$$

□

Proposition 1. — *Let V be a finite dimensional euclidean vector space, let S be a self-adjoint endomorphism of V and let π be a non zero orthogonal projector in V. Then follows*

$$\mathbf{Tr}(\exp(S)\pi) \geq \mathbf{rank}(\pi) \cdot \exp\left(\mathbf{Tr}(S\pi)/\mathbf{rank}(\pi)\right). \tag{4}$$

Proof. — Let $S = \sum_\lambda \lambda \cdot \pi_\lambda$ be the spectral decomposition of S. Then each of the idempotents π_λ is self-adjoint and $\exp(S) = \sum_\lambda \exp(\lambda) \cdot \pi_\lambda$. One computes

$$\mathbf{Tr}(S\pi) = \sum_\lambda \lambda \cdot \mathbf{Tr}(\pi_\lambda \pi) \text{ and } \mathbf{Tr}(\exp(S)\pi) = \sum_\lambda \exp(\lambda) \cdot \mathbf{Tr}(\pi_\lambda \pi). \tag{5}$$

Let ϑ denote the adjunction. The π_λ, and π, are self-adjoints and idempotents. Follows

$$\mathbf{Tr}(\pi_\lambda \pi) = \mathbf{Tr}(\pi_\lambda \pi_\lambda \pi\pi) = \mathbf{Tr}(\pi\pi_\lambda \pi_\lambda \pi) = \mathbf{Tr}(\vartheta(\pi_\lambda \pi)\pi_\lambda \pi) \geq 0 \tag{6}$$

by idempotency of π_λ and π, by cyclicity of $\mathbf{Tr}$, by self-adjointness of π_λ and π, and by positivity of $X \mapsto \mathbf{Tr}(\theta(X)X)$ respectively.

The sum $\sum_\lambda \mathbf{Tr}(\pi_\lambda \pi)$ has value $\mathbf{Tr}(\mathrm{Id}\pi) = \mathbf{Tr}(\pi) = \mathbf{rank}(\pi)$. The coefficients $\frac{\mathbf{Tr}(\pi_\lambda \pi)}{\mathbf{rang}(\pi)}$ are well defined, because π is assumed to be non zero, are positive, by (6), and have sum 1, as $\sum_\lambda \mathbf{Tr}(\pi_\lambda \pi) = \mathbf{rank}(\pi)$. From the convexity of the exponential function, one gets

$$\exp\left(\sum_\lambda \lambda \cdot \frac{\mathbf{Tr}(\pi_\lambda \pi)}{\mathbf{rank}(\pi)}\right) \leq \sum_\lambda \exp(\lambda) \cdot \frac{\mathbf{Tr}(\pi_\lambda \pi)}{\mathbf{rank}(\pi)}, \tag{7}$$

which, together with (5), yields inequality (4). □

Corollary 3.2. — *In situation of Theorem 3.1, for any p in P, $\pi_{\mathfrak{z}}(\rho(p))$ is expanding:*

$$\forall v \in V, \forall p \in P, \left\|\pi_{\mathfrak{z}}(\rho(p))\right\| \geq \|v\|. \tag{8}$$

Proof. — Indeed $\pi_{\mathfrak{z}}(\rho(p))$ can be diagonalized in an orthonormal basis with all diagonal coefficients greater than 1. □

3.1. Application. — *We consider the situation 2.2.1 and 2.2.2.*

Consider the adjoint representation Ad_ρ of G on $\mathfrak{gl}(V)$ by conjugation. Let $C(\mathrm{Ad}_\rho)$ be the vector space of functions on H generated by the matrix coefficients of Ad_ρ, ie by functions $\langle \phi, g\rangle : h \mapsto \phi(\rho(h) g \rho(h)^{-1})$ for g in $\mathfrak{gl}(V)$ and ϕ in its algebraic dual $\mathfrak{gl}(V)^\vee$. The function $\langle \phi, g\rangle$ depends linearly on both g and ϕ. Consequently $C(\mathrm{Ad}_\rho)$ is finite dimensional: its dimension is bounded by $\dim\left(\mathfrak{gl}(V) \otimes \mathfrak{gl}(V)^\vee\right)$.

The following identity has two consequences (compare with [**Bou60**] §7.1).

$$\langle \phi, g\rangle(h \cdot h') = \langle \phi, \rho(h') g \rho(h'^{-1})\rangle(h) \tag{9}$$

Firstly the matrix coefficients of Ad_ρ are globally stable under the action of H by translation: as a result we get a linear action of H on $C(\mathrm{Ad}_\rho)$. Secondly (10) readily express that, for a fixed ϕ in $\mathfrak{gl}(V)^\vee$ the map $g \mapsto \langle \phi, g\rangle$ is an equivariant morphism from $\mathfrak{gl}(V)$ to $C(\mathrm{Ad}_\rho)$.

Recall that H being *reductive in* G (see conventions), the restriction to H of a finite dimensional representation of G is semisimple (conventions, criterion b)). Consequently, in both $\mathfrak{gl}(V)$ and $C(\mathrm{Ad}_\rho)$ there is a unique isotypic projector onto the subspaces of invariant elements, namely onto the commutant $\mathfrak{z}$ of H in $\mathfrak{gl}(V)$, and onto the subset of constant functions (canonically isomorphic $\{0\}$ or $\mathbf{R}$ according to $\dim(V)$ being zero or not[(1)]). Moreover these projectors, say $\pi_\mathfrak{z}$ and $\pi_\mathbf{R}$ respectively, commute with any equivariant morphism. In particular, for the morphism $g \mapsto \langle \phi, g\rangle$ from $\mathfrak{gl}(V)$ to $C(\mathrm{Ad}_\rho)$, for any ϕ in $\mathfrak{gl}(V)^\vee$, we get

$$\pi_\mathbf{R}\left(\langle \phi, g\rangle\right) = \langle \phi, \pi_\mathfrak{z}(g)\rangle. \tag{10}$$

Theorem 3.3. *— We consider the situation 2.2.1 and 2.2.2.*

Let $C(\mathrm{Ad}_\rho)$ the vector space of functions on H generated by the matrix coefficients of Ad_ρ, let Ω be a nonempty subset of H, write $\pi_\mathbf{R}$ for the equivariant projector of $C(\mathrm{Ad}_\rho)$ onto constant functions. Set

$$c = \sup\{\pi_\mathbf{R}(f) \,|\, f \in C(\mathrm{Ad}_\rho), \sup_{\omega\in\Omega} |f(w)| \leq 1\}$$

so that, for any f in $C(\mathrm{Ad}_\rho)$, we have: $\sup_{\omega\in\Omega} |f(\omega)| \cdot c \geq |\pi_\mathbf{R}(f)|$.

Then

$$\forall e \in \mathfrak{gl}(V), \forall v \in V, \sup_{\omega\in\Omega} \left\| \rho\left(\omega^{-1}\right) \cdot e \cdot \rho\left(\omega\right)(v)\right\| \cdot c \geq \left\|\pi_\mathfrak{z}(e)(v)\right\|. \tag{11}$$

Proof. — First remark follows by homogeneity from definition of c.

Fix e in $\mathfrak{gl}(V)$, v in V, and denote by w the vector $\pi_\mathfrak{z}(e)(v)$. Applying Cauchy-Schwarz inequality in V, we get, for any ω in H,

$$\left\| \rho\left(\omega^{-1}\right) \cdot e \cdot \rho\left(\omega\right)(v)\right\| \cdot \|w\| \geq \left(\rho\left(\omega^{-1}\right) \cdot e \cdot \rho\left(\omega\right)(v) \,\middle|\, w\right) \tag{12}$$

(1) If $\dim(V) \neq 0$, then $\langle \mathbf{Tr}, \mathrm{Id}\rangle : h \mapsto \dim(V)$ is a nonzero constant matrix coefficient.

Note that the right-hand side, as a function of ω, is a matrix coefficient belonging to $C(\mathrm{Ad}_\rho)$. Consequently, by definition of c,

$$\sup_{\omega\in\Omega}\left(\rho\left(\omega^{-1}\right)\cdot e\cdot\rho\left(\omega\right)\left(v\right)|\,w\right)\cdot c\geq\pi_{\mathbf{R}}\Big(\left(\rho\left(\omega^{-1}\right)\cdot e\cdot\rho\left(\omega\right)\left(v\right)\big|\,w\right)\Big). \tag{13}$$

Formula (10) with $\phi : g\mapsto(\mathrm{Ad}_\rho(g)\cdot p(v)|w)$ and $g=p$ specialises in

$$\pi_{\mathbf{R}}\left(\left(\rho\left(\omega^{-1}\right)\cdot e\cdot\rho\left(\omega\right)\left(v\right)\big|\,w\right)\right)=\left(\pi_{\mathfrak{z}}(e)(v)\,|\,w\right)=\|w\|^2. \tag{14}$$

Applying $\sup_{\omega\in\Omega}$ to both sides of (12), combining with (13), substituting (14), we finally get

$$\sup_{\omega\in\Omega}\left\|\rho\left(\omega^{-1}\cdot p\cdot\omega\right)(v)\right\|\cdot\|w\|\cdot c\geq\|w\|^2, \tag{15}$$

which implies (11), as $\|w\|\geq 0$. □

Corollary 3.4. — *In situation of Theorem 3.3, assume moreover that*

(∗) *every matrix coefficient in* $C(\mathrm{Ad}_\rho)$ *that cancels on* Ω *actually cancels on whole* H.

Assuming (∗) *and* $\dim(V)>0$, *we get* $1\leq c\neq\infty$, *and*

$$\forall\, p\in\exp_G(\mathfrak{p}),\forall\, v\in V,\sup_{\omega\in\Omega}\left\|\rho\left(\omega^{-1}\cdot p\cdot\omega\right)(v)\right\|\geq\|v\|/c. \tag{16}$$

Proof. — Assuming $\dim(V)>0$, constant functions are matrix coefficients of Ad_ρ, hence $c\geq\pi_{\mathbf{R}}(1)=1$. Condition (∗) ensure that the map $f\mapsto\sup_{\omega\in\Omega}|f(w)|$ actually defines a *norm*, instead of a mere semi-norm, on the subspace of $C(\mathrm{Ad}_\rho)$ on which it takes finite values. By definition c is the operator norm of the restriction to this subspace of the bounded linear application $\pi_{\mathbf{R}}$. Whence $c<\infty$.

The inequality (16) follows from combining 3.3 and 3.1, and then dividing by c (which is positive and invertible.) □

Condition (∗) is satisfied for any Zariski dense subset Ω of H, and in particular[(2)] if Ω has nonempty interior or positive Haar measure. If moreover Ω is bounded, then the map $f\mapsto\sup_{\omega\in\Omega}|f(w)|$ defines a norm on whole of $C(\mathrm{Ad}_\rho)$. Note that condition (∗) means that the evaluation maps $f\mapsto\omega$, with ω in Ω, generate the algebraic dual of $C(\mathrm{Ad}_\rho)$. Extracting from this generating set a *base*, one can see that condition (∗) can still be met by replacing Ω by a subset of cardinality at most $\dim(C(\mathrm{Ad}_\rho))$. Note that in term of such a base, and a base of base of $C(\mathrm{Ad}_\rho)$ (which can be deduced from a base of V), one can effectively bound above the constant c in Corollary 3.4.

(2) Recall H is assumed to be connected, and being smooth, it is irreducible.

4. Proof of Theorem 1

We will show how to derive Theorem 1 from Corollary 3.4. Actually we will establish the following and more precise statement. The existence of Θ follows from criterion c) of the terminological conventions section.

Proposition 2. — *In the situation of theorem 1, let Θ be a Cartan involution of G under which H is globally invariant, and let K be the maximal projectively compact subgroup of G made of fixed points of Θ. Write $\mathfrak{g}$, $\mathfrak{z}_G$ and $\mathfrak{k}$ for the Lie algebras of G, $Z_G(H)$, and K respectively. Let $\mathfrak{p}$ be the orthocomplement $(\mathfrak{k}+\mathfrak{z}_G)^\perp$, for the Killing form on $\mathfrak{g}$, of the compositum of $\mathfrak{z}_G$ and $\mathfrak{k}$.*

Then the subset $Y = K \cdot \exp_G(\mathfrak{p})$ of G satisfies two conditions of theorem 1.

We will prove that Y satisfies each of these conditions in the next two subsections.

4.1. First condition. — Recall first another theorem of G. Mostow.

Theorem 4.1 **(Mostow,** [**Mos55b**] **Theorem 5)**. — *Let G be a connected semi-simple real Lie group and let K be a maximal projectively compact subgroup of G. Let $\mathfrak{g}$ denote the Lie algebra of G and $\mathfrak{k}$ the Lie algebra of K. Let $\mathfrak{z}$ be any Lie subalgebra of $\mathfrak{g}$. Orthogonality is understood with respect to the Killing form.*

Then the following application is a diffeomorphism.

$$\begin{array}{ccc} K \times \left(\mathfrak{k}^\perp \cap (\mathfrak{k}^\perp \cap \mathfrak{z})^\perp\right) \times \left(\mathfrak{k}^\perp \cap \mathfrak{z}\right) & \to & G \\ (k, P, Z) & \mapsto & k \cdot \exp_G(P) \cdot \exp_G(Z) \end{array} \tag{17}$$

Actually G. Mostow states that G "decomposes topologically", meaning that we have a homeomorphism. This is enough to establish first condition of Theorem 1, but one can check directly, as below, that map (17) is an immersion. As both sides of (17) have equal dimension, (17) will be a local diffeomorphism, but being bijective, it will be an (analytic) diffeomorphism. Let us prove that at each (k, P, Z) in $K \times \left(\mathfrak{k}^\perp \cap (\mathfrak{k}^\perp \cap \mathfrak{z})^\perp\right) \times \left(\mathfrak{k}^\perp \cap \mathfrak{z}\right)$ the tangent map is injective.

Proof. — Left and right translating one is reduced to the case where $Z = 0$ and $k = \exp_G(0)$. Write $p = \exp_G(P)$, and let dK, dP and dZ be arbitrarily small in $\mathfrak{k}$, $\mathfrak{p}$ and $\mathfrak{k}^\perp \cap \mathfrak{z}$ respectively. At first order, $\exp_G(dK)\exp_G(P + dP)\exp_G(dY) \simeq p \cdot (p^{-1}\exp_G(dK)p)\exp_G(dP)\exp_G(dY)$. The latter equals $p \cdot \exp_G(\mathrm{Ad}_{p^{-1}}(dK))\exp_G(dP)\exp_G(dY)$, or, up to first order,

$$p \cdot \exp_G(\mathrm{Ad}_{p^{-1}}(dK) + dP + dY).$$

We will be done showing that $\mathrm{Ad}_{p^{-1}}(dK) + dP + dY$ cannot be zero for arbitrarily small and not simultaneously zero dK, dP and dZ, namely that $\mathrm{Ad}_{p^{-1}}(\mathfrak{k})$, $\left(\mathfrak{k}^\perp \cap (\mathfrak{k}^\perp \cap \mathfrak{z})^\perp\right)$ and $\mathfrak{k}^\perp \cap \mathfrak{z}$ are in direct sum. Note that $\mathfrak{k}$ and $\mathfrak{k}^\perp$ are anisotropic of opposite sign (negative and positive resp.). By invariance of the Killing form,

$\mathrm{Ad}(\exp_G(P))(\mathfrak{k})$ is negative (cf. 2.1.1), hence has intersection $\{0\}$ with $\mathfrak{k}^\perp$. Consequently $\mathrm{Ad}_{p^{-1}}(\mathfrak{k})$ and $\mathfrak{k}^\perp$ are in direct sum. As $\mathfrak{k}^\perp$ is anisotropic, $\mathfrak{z} \cap \mathfrak{k}^\perp$ is supplementary to its orthogonal in $\mathfrak{k}^\perp$. □

Let K and Y be as in proposition 2. Applying theorem 4.1 to $\mathfrak{z} = \mathfrak{z}_\mathfrak{g}$, it follows that the equality $G = Y \cdot Z_G(H)^0$ is satisfied and that Y defines a closed subvariety inside G. In particular Y satisfies condition 1 of theorem 1.

Note that the fact that $Z_G(H)$ is invariant under Θ is equivalent to the fact that $\mathfrak{z}_\mathfrak{g}$ is generated by $\mathfrak{k} \cap \mathfrak{z}_\mathfrak{g} \oplus \mathfrak{k}^\perp \cap \mathfrak{z}_\mathfrak{g}$. For more general maximal projectively compact K, $\mathfrak{k}^\perp \cap \mathfrak{z}_\mathfrak{g}$ can have lesser dimension. Consequently Y will get bigger; this suggest that the hypothesis on K in proposition 2 is necessary.

4.2. Second condition. — What is left, in order to prove Proposition 2, is to show that Y satisfies the condition 2 of the theorem 1. Fix ρ as in theorem 1. We will prove formula 1 under a weaker hypothesis on Ω, namely condition $(*)$ page 77.

Proof. — If $\dim(V) = 0$, formula (1) is immediate. So assume $\dim(V) > 0$.

Note that it is enough to prove formula (1) for any subset Ω_b of Ω instead of Ω. Moreover, according to remarks following Corollary 3.4, we can assume this subset to be finite and still satisfy condition $(*)$. In particular such an Ω_b will be bounded.

Because V is finite dimensional, all norms on V are equivalent. Consequently, the validity of formula (1) doesn't depend on the chosen norm on V, if one allows to change the constant. In particular one can assume that this norm is associated to a euclidean structure on V with respect to which .... In particular such a norm is K-invariant.

Note that we are in situation 2.2.1 and 2.2.2. Recall (proposition 2) that $Y = K \cdot P$. As the euclidean norm on V is K invariant, inequality (1) for y in Y will follow from inequality (1) for y in P.

We wish to prove that there exists a constant $c > 0$ such that

$$\forall\, y \in P, \forall\, v \in V, \sup_{\omega \in \Omega} \left\| \rho(y \cdot \omega)(v) \right\| \geq c \cdot \|v\|\,. \tag{18}$$

As Ω is bounded, $C = \sup_{\omega \in \Omega_b} \left|\left|\left| \omega^{-1} \right|\right|\right|$ is finite, and because $\dim(V) > 0$, C is positive and invertible. Because of the inequalities

$$\left\| \rho\left(\omega^{-1} \cdot p \cdot \omega\right) v \right\| \leq \left|\left|\left| \rho\left(\omega^{-1}\right) \right|\right|\right| \cdot \left\| \rho\left(p \cdot \omega\right) v \right\| \leq C \cdot \left\| \rho(p \cdot \omega) v \right\|,$$

formula (18) follows from

$$\forall\, y \in P, \forall\, v \in V, \sup_{\omega \in \Omega} \left\| \rho(\omega^{-1} \cdot y \cdot \omega)(v) \right\| \geq \frac{c}{C} \cdot \|v\|\,. \tag{19}$$

Let c' be the constant of Theorem 3.3. According Corollary 3.4 formula (19), and hence (18) hold for $\frac{c}{C} = \frac{1}{c'}$. □

Proposition 2 and Theorem 1 are proved, with Y given by 2 (or 2.2.1), assuming only that Ω satisfies condition $(*)$, and, whenever the norm on V is given by 2.2.2, with the constant

$$\frac{C}{c'} = \frac{\sup_{\omega\in\Omega_b} |||\omega^{-1}|||}{\sup\{\pi_{\mathbf{R}}(f) | f \in C(\mathrm{Ad}_\rho), \sup_{\omega\in\Omega_b} |f(w)| \leq 1\}}. \tag{20}$$

5. Postliminary enhancements: case of reductive G

Actually, Theorem 1 can be generalised a bit. Since such hypotheses do not harmonises well with our proof, we show to generalise 1 in a separate section.

First of all, if G is a linear Lie group, one can consider the algebraic structure (given by the algebra of matrix coefficients). In this case the theorem 1 and its proof remain true if one only assume that (the Zariski closure of) H is Zariski connected, instead of connected (as a Lie group).

Note that, for any compact subset C of G, if we replace Y by CY, the conclusion of Theorem 1 still hold, up to a change in the constant c. This remark shows that we can allow G to have finiely many connected components in Theorem 1.

More importantly,

Lemma 5.1. — *In Theorem 1, G can be allowed to only be reductive* Lie *group. We then ask H to be a connected* reductive subgroup in G*, meaning that the adjoint action of H on $\mathfrak{g}$ is completely reducible. We do not even ask for the representation ρ of G to be semisimple.*

Proof. — Let Z denote the center of G and $[G,G]$ be the derived subgroup of G. Set $H' = (HZ) \cap [G,G]$. Note that H' is reductive in $[G,G]$, because it has the same action as H on $\mathfrak{g}$ and because $[\mathfrak{g},\mathfrak{g}]$ is invariant subspace of $\mathfrak{g}$. We can apply Theorem 1 to H' in $[G,G]$, in order to get a subset Y' of $[G,G]$. As $Z_G(H) = Z_G(HZ) = Z_{[G,G]}(H')Z$, we have $Y'Z_G(H) = Y'Z_{[G,G]}(H')Z = [G,G]Z = G$. Thus Y as a subset of G satisfies the first condition of theorem 1, with respect to G and H.

Let us check that Y also satisfies the second condition of theorem 1, namely formula (1). First note we can replace Ω by a bounded subset, then that, for any bounded subset C of Z, formula (1) still holds, up to a change in constant, if we replace Ω by ΩC, and conversely. Consequently we can replace H by HZ and assume Ω to have nonempty interior in HZ. Taking a smaller subset we can assume Ω, which we assumed to be bounded, is a product in G of subsets of $[G,G]$ and Z. Using the converse above, we can replace HZ by H' and assume Ω, to be contained in H' and have nonempty interior in H'. □

Appendix A
Further remarks

A.1. One issue. — Consider, as in [**EMS97**] a real algebraic Lie group G with arithmetic lattice Γ, a connected Lie subgroup H in G and denote by $\pi : G \to \Gamma\backslash G$ the quotient map. The original proof of Theorem 1.1 in [**EMS97**] uses some auxiliary map $\Theta : \mathbf{R}^{\dim(H)} \to H$.

What is actually proved, in [**EMS97**], is the following (see formula (23) in [**EMS97**]). Let λ be the standard Lebesgue measure on $\mathbf{R}^{\dim(H)}$. Consider, for any ball J in $\mathbf{R}^{\dim(H)}$, the restriction λ_J of λ to J, and its direct image $(\pi\circ\Theta)_\star\lambda_J$ by the composite map of Θ and π. Then [**EMS97**] proves, under the hypotheses of its Theorem 1.1, that

(21) the family of translated measures $((\pi\circ\theta)_\star\lambda_J\cdot g)_{g\in G}$ is a *narrow familly*

(see [**EMS97**] formula (23)) in the set of bounded measures on $\Gamma\backslash G$.

In [**EMS97**], right before their formula (23), the authors claim that: the fact that

(22) the familly of translated measures $(\mu_H\cdot g)_{g\in G}$ is a narrow familly

is a consequence of what is actually proved, the fact (21) emphasised above (assuming H has a closed orbit $\Gamma\backslash\Gamma H$ in $\Gamma\backslash G$, that this orbit supports an H-invariant probability μ_H and assuming the hypotheses of [**EMS97**], Theorem 1.)

A.2. Two strategies. — We see two strategies to justify such a claim: either to approach H by a the image of big enough ball; or to approach H by a cover of bounded degree and made of images, by Θ, of balls from $\mathbf{R}^{\dim(H)}$. First strategy require Θ to be (almost) surjective: this is unclear whether this is the case. For the second strategy we may also consider translates of images of balls, but we need to be able to apply some Besicovich covering property, for example as in the form written in [**KT07**] §1.1, for these images of balls and possibly their translates.

We point out that the setup from the recent [**KT07**] allows to consider a wider class of functions Θ. In a subsequent article, we will indeed show how to combine our Theorem 1 with results of [**KT07**] to obtain genralisations of the main result of [**EMS97**]. From now on, we will base ourselves on the setup from [**EMS97**]. Below we will apply the first strategy above to deduce (22) from a variant modification of (21). but prior let us, in the following section, modify Θ.

A.3. Three parametrisations. — Following [**EMS97**], Introduction, first line, we assume that H is assumed to be a connected real algebraic Lie subgroup of G. We make the following claim, that we prove below: *for some dimension N and some parameters n and Λ, there exists a surjective analytic map $\Theta_H : \mathbf{R}^N \to H$ belonging to some of the classes from Definition 3.1 of* [**EMS97**]*, say class $E_G(N_H, n_H, \Lambda_H)$.*

Recall this denotes the class of (measurable) maps from $\mathbf{R}^{N_H}$ to H whose matrix coefficients, in the adjoint representation of G, may be written as linear combination of products of a monomial of degree at most n_H by an exponential of a complex linear form with coefficients of norm at most to Λ_H (inclusive). We now turn to the proof of the claim we made in the present subsection A.3.

Proof. — Recall that H is assumed to be a connected reductive real algebraic Lie group. Let us first consider special cases.

A.3.1. Assume H is a connected Lie torus A of G. — In this case the exponential map, written in some basis of the Lie algebra, is surjective and belongs $E_G(N_A, n_A, \Lambda_A)$, with $N_A = \dim(A)$, with Λ_A depending on a choice of a basis of the Lie algebra and the weights of A in the adjoint representation of G, and with n_A depending on the maximal multiplicities of these weights; Actually, as we assumed H to be *reductive in* G, the adjoint action of A on $\mathfrak{g}$ is semisimple, hence $n_A = 0$.

A.3.2. Assume H is a connected compact group K of G. — The image of the map Θ of [**EMS97**] contain some open neighbourhood U of identity. Let us show that *there is an integer M_U such that every element of K can be written as a M-th power of some element in U.*

Proof. — First note that U contain a neighboorhood of identity which is stable under conjugation. Indeed $K \smallsetminus U$ is closed in K, hence compact; as a result its saturation under conjugation by K is a compact which does not contain the neutral element; the seeked neighboorhood is the complement of this compact in K. We may replace U by this smaller neighborhood. Then recall that every element of K is contained in a connected maximal torus, and that these tori are conjugated. Consequently we can assume K itself is a compact connected torus. The latter case can be worked explicitely. □

Consequently, the map Θ_K from $\mathbf{R}^{\dim(K)}$ to K which sends x to $\Theta(x)^M$ is surjective. Note that if, written in some basis, Θ belongs to $E_G(n, m, \Lambda)$, then Θ_K, written in the same basis, belongs to $E_G(M \cdot n, M \cdot m, M\Lambda)$.

A.3.3. Turn now to the general case of a reductive subgroup H in G. — Let K and A denote a maximal compact subgroup and the connected component of a split Cartan subgroup in H. Considers the maps Θ_A and Θ_K obtained in the previous cases, and let Θ_H be the map from $\mathbf{R}^k \times \mathbf{R}^a \times \mathbf{R}^k$ to H which sends (x, y, z) to $\Theta_K(x) \cdot \Theta_K(y) \cdot \Theta_K(z)$. From the decomposition $H = KAK$ we deduce that Θ_H is surjective. As Θ belongs to it is enough to consider the case of a connected subtorus of G and the case of a connected compact subgroup of G. As the parametrisations of K and A belongs to classes $E_G(N_K, n_K, \Lambda_K)$ and $E_G(N_A, n_A, \Lambda_A)$ respectively , the map Θ_H belongs to class $E_G(N_A + 2N_K, n_A + 2n_K, \Lambda_A + 2\Lambda_K)$.

We justified the claimed of this this section A.3, with for $N_H = N_A + 2N_K$, $n_H = n_A + 2n_K$, $\Lambda_H = \Lambda_A + 2\Lambda_K$. □

A.3.4. Let us indicate how to generalise this for connected real algebraic Lie subgroups H of G which are non necessarily reductive. As such a H is linear, it is an almost semi-direct product of its unipotent radical and some Levi subgroup. As a result we only need to consider the reductive case and the unipotent case. The

reductive case is already considered above. In the unipotent case, every representation is triangularisable (over **C**) and the exponential map, written in some basis of the (real) Lie algebra, has manifestly matrix coefficients which are polynomials maps. It will be enough to show that the exponential map is surjective. Fix a faithfull linear representation, so that the exponential map write as a polynomial map, whose reciprocal is given by the taylor series at 1 of the logarithm, which converges on unipotent matrices. The exponential map, being invertible is surjective.

A.4. Four steps. — Consider an analytic map Θ_H as in section A.3. We saw how to construct such a map, at least non effectively. We will justify the claim of [**EMS97**] for this map Θ_H instead of the original Θ.

Let us first indicate why such a change does not impact the proof of Theorem 1.1 in [**EMS97**]. As Θ_H belongs to some class $E_G(N_H, n_H, \Lambda_H)$, the proof of [**EMS97**] still holds between formulas (23) and (24): one can apply Theorem 3.9 and Corollary 3.10 of [**EMS97**]. Then comes the part of the proof where, following our section 1, one wish to apply our Theorem 1.1 instead of Proposition 4.4 of [**EMS97**], seeking to contradict formula (24). In order to apply our Theorem 1, we need to verify that, *for any nonempty open ball J in $\mathbf{R}^{N_H}$, the subset $\Omega = \Theta_H(J)$ of H satisfies our hypothesis, namely having nonempty interior.*

Proof. — We know that Θ_H is analytic and surjective. Hence its set of critical points is a proper subvariety, and, as $\mathbf{R}^{N_H}$ is equidimensional, it has everywhere nonzero codimension, hence has empty interior. As J has nonempty interior, it contains a nonempty open subset of regular points. But Θ is submersive, hence open, on the regular locus. □

Let us now turn, finally, to the proof of the claim of [**EMS97**] for Θ_H. We come back to the notations of the section A.1. We first prove that $(\pi \circ \Theta_H)_\star \lambda_J$ may be written $F_J \cdot \mu_H$, where F_J is a measurable and summable function on $\Gamma\backslash G$ with compact support $\pi \circ \Theta_H(J)$.

Proof. — By virtue of Radon-Nikodym theorem, one only needs to show that $(\pi \circ \Theta_H)_\star \lambda_J$ is absolutely continuous with respect to μ_H. Let E be a null set for μ_H. As π is a covering, the inverse image of a null set of μ_H is a null set of the Haar measure on H. It will be enough to show that the inverse image by Θ_H of a null set E for this Haar measure is a null set for λ. As the critical locus of Θ_H is a null set (actually an analytic subvariety), we may replace Θ_H and λ by their restriction to the regular locus of Θ_H. To prove that $\Theta_H^{-1}(E)$ is a null set we may work locally, that is in restriction to a sufficiently small ball (in the regular locus). As Θ_H is a submersion, we may suppose that it is a trivial fibration on wich λ is equivalent to the product measure. This last case is obvious. □

The inference (21) ⇒ (22) can be formulated as follows. Knowing that, for any ball J in $\mathbf{R}^{N_H}$, the family $((\pi \circ \Theta_H)_\star \lambda_J \cdot g)_{g \in G}$ is narrow, we want to show that the

family $(\mu_H \cdot g)_{g\in G}$ is narrow. We will actually show that, *given any subset* Y of G, if, for any ball J in $\mathbf{R}^{N_H}$, the family $((\pi\circ\Theta_H)_\star \lambda_J \cdot y)_{y\in Y}$ is narrow, then the family $(\mu_H \cdot y)_{y\in Y}$ is narrow.

For any ϵ in $\mathbf{R}$, let $1_{\geq\epsilon}$ the characteristic function of the unbounded closed interval in $\mathbf{R}$ which starts at ϵ. We will consider the following families. The first three are relative to some nonempty open ball J of $\mathbf{R}^{N_H}$.

1. $((F_J\mu_H)\cdot y)_{y\in Y}$,
2. $((F_J 1_{\geq\epsilon}(F_J)\mu_H)\cdot y)_{y\in Y}$, relative to $\epsilon > 0$,
3. $((1_{\geq\epsilon}(F_J)\mu_H)\cdot y)_{y\in Y}$, relative to $\epsilon > 0$,
4. $((1_{\geq 0}(F_J)\mu_H)\cdot y)_{y\in Y}$,
5. $((\mu_H)\cdot y)_{y\in Y}$.

By definition $((F_J\mu_H)\cdot y)_{y\in Y} = ((\pi\circ\Theta_H)_\star\lambda_J\cdot y)_{y\in Y}$. By hypothesis the latter familly is narrow, so is the first. Our goal is to prove that family 5 is narrow. This will be done in four steps: we will prove that all above families are narrow, from famillies 2 to family 5.

Proof. — Note that $F_J 1_{\geq\epsilon}(F_J) \leq F_J$. As a result family 2 is dominated by family 1 elementwise. Hence family 2 is narrow.

Analogously, from the observation that $1_{\geq\epsilon}(F_J) \leq \frac{1}{\epsilon} F_J 1_{\geq\epsilon}(F_J)$ we conclude that families 2 dominate families 3, and consequently that families 3 are narrow.

Note that $1_{\geq\epsilon}(F_J)$ monotonously converges to $1_{\geq 0}(F_J)$ as ϵ approach 0 by positive values. Set $u(\epsilon) = \mu(1_{\geq 0}(F_J) - 1_{\geq\epsilon}(F_J))$. By Lebesgue's monotonous convergence theorem, $\lim_{\epsilon\to 0^+} u(\epsilon_0) = 0$. Note that, *independently of* y *in* Y, the (positive) measure

$$1_{\geq 0}(F_J)\mu_H - 1_{\geq\epsilon}(F_J)\mu_H$$

has mass $u(\epsilon)$. Hence narrowness of family 3 implies narrowness of family 4.

Consider an increasing covering family of nonempty open balls J in $\mathbf{R}^{N_H}$. As Θ_H is surjective, the image of this family by Θ_H will be a covering increasing family. Equivalently, $1_{\pi\circ\Theta_H(J)}$ will converge monotonously to the characteristic function $1_{\pi(H)}$ of $\pi(H)$. Consequently, as before, narrowness of $((1_{\pi\circ\Theta_H(J)}\mu_H)\cdot y)_{y\in Y}$ will imply narrowness of family 5. But, by definition of F_J, $1_{\pi\circ\Theta_H(J)}\mu_H = 1_{\geq 0}(F_J)\mu_H$. Thus family $((1_{\pi\circ\Theta_H(J)}\mu_H)\cdot y)_{y\in Y}$ equals family 4, and is narrow. Thus family 4 is indeed narrow. This finishes our proof. □

References

[Bou] N. BOURBAKI – *Éléments de mathématique. XXVI. Groupes et algèbres de Lie. Chapitre 3.*

[Bou60] ———, *Éléments de mathématique. XXVI. Groupes et algèbres de Lie. Chapitre 1: Algèbres de Lie*, Actualités Sci. Ind. No. 1285. Hermann, Paris, 1960.

[EMS97] A. ESKIN, S. MOZES & N. SHAH – "Non-divergence of translates of certain algebraic measures", *Geom. Funct. Anal.* **7** (1997), no. 1, p. 48–80.

[Hel78] S. HELGASON – *Differential geometry, Lie groups, and symmetric spaces*, Pure and Applied Mathematics, vol. 80, Academic Press Inc. [Harcourt Brace Jovanovich Publishers], New York, 1978.

[KT07] D. KLEINBOCK & G. TOMANOV – "Flows on S-arithmetic homogeneous spaces and applications to metric Diophantine approximation", *Comment. Math. Helv.* **82** (2007), no. 3, p. 519–581.

[Mos55a] G. D. MOSTOW – "Self-adjoint groups", *Ann. of Math. (2)* **62** (1955), p. 44–55.

[Mos55b] _____, "Some new decomposition theorems for semi-simple groups", *Mem. Amer. Math. Soc.* **1955** (1955), no. 14, p. 31–54.

RODOLPHE RICHARD, IRMAR, Bâtiment 22-23, université de Rennes 1, Campus de Beaulieu, 35000 Rennes. • *E-mail :* Rodolphe.RICHARD@Normalesup.org

NIMISH SHAH

RÉSULTAT GÉOMÉTRIQUE SUR LES REPRÉSENTATIONS DE GROUPE RÉDUCTIFS SUR UN CORPS ULTRAMÉTRIQUE

par

Rodolphe RICHARD

Table des matières

1. Hypothèses et Énoncé 2
2. Notations 4
3. Propositions 7
4. Démonstration 11

Annexe 12
Appendice A. Variétés algébriques affines 13
Appendice B. Groupes algébriques affines, linéaires, réductifs . . . 15
Appendice C. Corps locaux ultramétriques 17
Appendice D. Espace analytique 19
Appendice E. Immeuble euclidiens de Bruhat-Tits 24
Appendice F. Convexité 26
Références 30

Cette article adapte les résultats de [**RS09**] au cas d'un groupe algébrique semi-simple G sur un corps local $\mathbf{k}$ muni d'une valeur absolue ultramétrique $|-|$.

Nous suivons, dans les grandes lignes, la méthode développée dans [**RS09**] pour le contexte archimédien (dont nos proposition 3.1 à 3.4 reprennent certains arguments). Pour pallier l'absence du théorème de décomposition de Mostow ([**Mos55**]) pour $G(\mathbf{k})$ et la propriété de convexité de la fonction exponentielle, qui n'est plus partout définie, nous considérons le plongement $\Theta : \mathscr{I}_{\mathbf{k}}(G) \to G^{\mathrm{an}}$, de *l'immeuble de Bruhat-Tits* $\mathscr{I}_{\mathbf{k}}(G)$ de G sur $\mathbf{k}$ dans *l'espace analytique* G^{an}, au sens de Berkovich, associé à G.

Notre démonstration repose en effet sur le Théorème F.3 de l'annexe, qui se base sur les travaux de Bertrand Rémy, Amaury Thuillier et Anette Werner dans [**RTW09**]. Ces auteurs généralisent une construction du chapitre 5 de [**Ber90**], où V. Berkovich se restreint au cas des groupes de Chevalley (semi-simples déployés). Le Théorème F.3 met à profit les propriétés de convexité de $\mathscr{I}_{\mathbf{k}}(G)$, et remplace la propriété de convexité de la fonction exponentielle de [**RS09**] par la convexité de fonctions de la forme $x \mapsto |f(x)|$ (Prop. 3.6).

La décomposition de Mostow est remplacée par la décomposition moins précise du Théorème F.1 et sa conséquence au corollaire 2.1. Pour obtenir l'énoncé 2.1, notre démonstration utilise l'existence de points fixes pour l'action de groupes d'isométries compacts sur les immeubles de Bruhat-Tits. Ces propriétés découlent de l'existence de métriques hyperboliques, et justifient le choix de la géométrie ultramétrique au sens de Berkovich, qui permet de considérer des espaces métriques complets.

Que Bertrand Remy, Amaury Thuillier et Georges Tomanov reçoivent ici mes remerciements pour leur accueil chaleureux et leur conversation enrichissante à l'occasion de mon déplacement à l'institut Camille Jordan de l'université Lyon 1 Claude Bernard.

C'est en cotoyant, à l'IRMAR, Antoine Chambert-Loir, Antoine Ducros et Jérôme Poineau que j'ai pu me familiariser avec les espaces de Berkovich. Que cet article leur témoigne de ma reconnaissance.

1. Hypothèses et Énoncé

Par convention, *un groupe algébrique linéaire*, et plus généralement un sous-groupe algébrique linéaire, est supposé *affine de type fini*, *réduit* et *connexe*. La nécessité de ces hypothèse n'a pas été vérifiée : notons que, comme notre résultat principal ne concerne que les groupes de points rationnels, il peut s'appliquer aux groupes non réduits, quitte à passer au sous-groupe réduit associé. Remarquons aussi que, dans un groupe algébrique linéaire, le centralisateur d'un sous-groupe algébrique linéaire n'est pas toujours réduit. Par exemple, en caractéristique non nulle p, le centre de $SL(p)$ est connexe, de dimension 0 mais a une algèbre de Lie non nulle.

Soit G un groupe algébrique linéaire sur un corps $\mathbf{k}$. Étant donnée une représentation linéaire de degré fini $\rho : G \to GL(V)$, on notera $\mathrm{Ad}_\rho : G \to GL(\mathfrak{gl}(V))$ l'action par conjugaison G sur $\mathfrak{gl}(V)$.

(1) Pour g dans G, $\mathrm{Ad}_\rho(g)$ envoie e sur $\rho(g)e\rho(g)^{-1}$.

Pour tout sous-groupe algébrique linéaire H de G, on notera $C_H\left(\mathrm{Ad}_\rho\right)$ l'espace vectoriel sur $\mathbf{k}$ engendré par les coefficients matriciels de l'action de H sur $\mathfrak{gl}(V)$. L'espace $C_H\left(\mathrm{Ad}_\rho\right)$ est formé de fonctions régulières sur H. Étant donné un ensemble Ω de points de H, nous considérons la propriété suivante.

$(*)$ Tout coefficient matriciel de Ad_ρ qui s'annule sur Ω s'annule en fait sur H.

Cette propriété est notamment vérifiée si Ω est Zariski dense dans H. Mettons en exergue deux autres conditions sur le H-module V.

$(**)$ L'action ρ de H sur V est telle que V^H, le plus grand sous-module de points fixes, a un unique supplémentaire H-stable.

$(**)'$ En surcroît de $(**)$, ce supplémentaire de V^H, comme représentation de H, n'a pas de quotient isomorphe à la représentation triviale.

La condition $(**)$ revient à supposer que V ne contient pas d'extension non triviale *de* la représentation triviale, et la condition $(**)'$ que V ne contient pas non plus d'extension non triviale *par* la représentation triviale. Les conditions $(**)$ et $(**)'$ sont automatiquement vérifiées si le H-module V est semi-simple. C'est le cas si H est réductif et le corps $\mathbf{k}$ de caractéristique nulle.
Remarques :
i) Lorsque la condition $(**)$ est vérifiée, le supplémentaire H-stable de V^H est le noyau d'un *unique* projecteur H-équivariant de V sur V^H (le *projecteur de Reynolds*, cf. [**Dem76**]). Étant donné un morphisme H-équivariant $\Phi : V \to W$ entre deux H-modules V et W satisfaisant $(**)$, ce morphisme commute aux projecteurs sur le lieu fixe si V satisfait la condition $(**)'$.
ii) En revanche, en caractéristique non nulle p, l'action adjointe de $GL(p)$ sur $\mathfrak{gl}(p)$ ne vérifie pas la condition $(**)$. Le sous-espace fixe est la droite $\mathbf{k}\cdot\mathrm{Id}$ formée des homothéties. Or cette droite n'a pas de supplémentaire stable : c'est déjà le cas pour l'action des matrices de permutation sur le sous-espace diagonal. Lorsque p est impair, l'action induite de $GL(p)$ sur $\frac{\mathfrak{gl}(p)}{\mathbf{k}\cdot\mathrm{Id}}$ satisfait la condition $(**)$ car il n'y a pas d'élément invariant non nul (cf.[**Bou60**], §6, Exercice 24). Elle ne satisfait pas la condition $(**')$ car l'action quotient sur $\frac{\mathfrak{gl}(p)}{\mathbf{k}\cdot\mathrm{Id}} \Big/ \frac{\mathfrak{sl}(p)}{\mathbf{k}\cdot\mathrm{Id}}$ est triviale.

Notre résultat principal est le suivant. Pour motiver cet énoncé nous renvoyons à [**RS09**] et [**Ric09**].

Théorème 1.1. — *Soit $(\mathbf{k},|-|)$ un corps local normé ultramétrique, soit G un groupe algébrique linéaire semisimple connexe sur $\mathbf{k}$, et soit H un sous-groupe réductif dans G. Notons Z le centralisateur de H dans G. Alors il existe une partie Y de $G(\mathbf{k})$, fermée pour la topologie ultramétrique, et telle que*

1. *d'une part on ait $G(\mathbf{k}) = Y \cdot Z_G(H)(\mathbf{k})$,*
2. *d'autre part, étant donnés*
   - *une représentation linéaire $\rho : G \to GL(V)$ de degré fini et définie sur $\mathbf{k}$, telle que les H-module $\mathfrak{gl}(V)$ et $C_H\left(\mathrm{Ad}_\rho\right)$ satisfassent $(**)$, et que $\mathfrak{gl}(V)$ satisfasse $(**)'$,*
   - *une partie non vide Ω de $H(\mathbf{k})$ ayant la propriété $(*)$,*
   - *une norme $\|-\|$ sur V, supposée homogène relativement à $|-|$,*

il existe une constante $c > 0$ telle que

$$\forall y \in Y, \forall v \in V, \sup_{\omega \in \Omega} \left\| \rho(y \cdot \omega)(v) \right\| \geq \|v\| / c. \tag{2}$$

Fixons ρ. L'inégalité (2) est vérifiée pour toute constante c lorsque le vecteur v est nul. Le théorème est donc vérifié, avec $Y = G(\mathbf{k})$, si V est de dimension nulle. *Dorénavant nous supposerons que la représentation ρ a un degré non nul.* En particulier les fonctions constantes sont des coefficients matriciels. En effet, tout coefficient diagonal de $g \mapsto \mathbf{Tr}\left(\mathrm{Ad}_\rho(g)\mathrm{Id}_V\right)$ vaut la constante 1. Ainsi $C_G\left(\mathrm{Ad}_\rho\right)$ et $C_H\left(\mathrm{Ad}_\rho\right)$ seront non nuls. Dans ce cas, la non vacuité de Ω découle de la condition $(*)$.

Remarquons que pour établir la formule (2), on peut remplacer Ω par un sous-ensemble Ω_b de Ω, car cela a pour effet de diminuer le membre de gauche de l'inégalité, sans modifier le membre de droite. Montrons que, comme Ω satisfait $(*)$, il existe un sous-ensemble fini Ω_b de Ω satisfaisant la propriété $(*)$.

Démonstration. — La condition $(*)$ signifie que lorsque ω décrit Ω, les morphismes d'évalution $f \mapsto f(\omega)$, définis sur $C_H\left(\mathrm{Ad}_\rho\right)$, engendrent le dual algebrique $C_H\left(\mathrm{Ad}_\rho\right)^\vee$ de $C_H\left(\mathrm{Ad}_\rho\right)$. Comme V est de dimension finie, $C_H\left(\mathrm{Ad}_\rho\right)$, qui est un quotient de $\mathfrak{gl}(V) \otimes \mathfrak{gl}(V)^\vee$, est de dimension finie. Il suffit donc d'extraire de la famille génératrice précédente une base, nécessairement finie, et de choisir pour Ω_b un sous-ensemble fini de Ω paramétrant cette base. □

Dorénavant Ω sera supposé borné dans $H(\mathbf{k})$.

Notre démonstration utilise les énoncés F.3 et F.1 de l'annexe, auquel nous renvoyons pour les définitions et conventions utilisées, en particulier concernant la notion de convexité telle que définie dans la section F. Pour plus d'approfondissement, on pourra également consulter [**RTW09**], ainsi que [**Ber90**] (chapitre 5) pour le cas des groupes semisimples déployés (« de Chevalley »).

Dans la section suivante, nous rappelons la situation et fixons les notations utilisées jusque la fin de la démonstration. Nous y explicitons en particulier la partie Y. La première conclusion du Théorème 1.1 résulte de la proposition 2.1, que nous déduisons de l'énoncé F.1. Nous énonçons également, avec la Proposition 2.2, une variante effective de la seconde conclusion du Théorème 1.1 pour la partie Y construite.

Dans la section 3, nous réunissons quelques énoncés indépendants qui seront utilisés dans la démonstration de la Proposition 2.2. Les énoncés 3.1 à 3.4 reprennent des arguments de [**RS09**]. La démonstration de l'énoncé de la proposition 3.6 repose sur l'énoncé F.3 de la première partie. Le cœur de la démonstration de la Propostion 2.2 occupe la section 4.

2. Notations

Rappelons la situation. Nous désignons par $\mathbf{k}$ un corps local muni d'une valeur absolue ultramétrique $|-|$, par G un groupe algébrique linéaire semi-simple sur $\mathbf{k}$, par H un sous-groupe réductif, et notons $Z_G(H)$ le centralisateur de H dans G, vu comme groupe algébrique affine non nécessairement réduit. Notons que $Z_G(H)$ n'interviendra toutefois que *via* son groupe $Z_G(H)(\mathbf{k})$ des points rationnels.

Nous nous sommes fixés $\rho : G \to GL(V)$, une représentation linéaire de G de degré fini non nul et définie sur $\mathbf{k}$ et $\|-\| : V \to \mathbf{R}$ une norme $(\mathbf{k},|-|)$-homogène sur V. Nous notons $\mathfrak{gl}(V)$ l'algèbre de Lie des endomorphismes de V, et Ad_ρ la représentation adjointe (1) de G sur $\mathfrak{gl}(V)$. Le sous-G-module de $\mathbf{k}[G]$ engendré par les coefficients matriciels de Ad_ρ est noté $C_G\left(\mathrm{Ad}_\rho\right)$, et le H-module formé de la restriction à H de ses fonctions régulières est noté $C_H\left(\mathrm{Ad}_\rho\right)$.

Nous désignons par Ω une partie bornée non vide de $H(\mathbf{k})$ sur laquelle aucune fonction régulière non nulle sur H issue de $C_H\left(\mathrm{Ad}_\rho\right)$ ne s'annule identiquement.

Notons $\mathfrak{z}$ le centralisateur de H dans $\mathfrak{gl}(V)$. D'après l'hypothèse $(**)$ pour Ad_ρ, il existe un unique projecteur H-équivariant de $\mathfrak{gl}(V)$ sur $\mathfrak{z}$ (cf. Remarque *i)*). Comme V est de dimension non nulle, les coefficients diagonaux de $h \mapsto \mathrm{Ad}_\rho(h)(\mathrm{Id}_V)$ forment un coefficient matriciel constant non nul de Ad_ρ. Ainsi, le sous-module fixe de $C_H\left(\mathrm{Ad}_\rho\right)$ est le sous-module formé des fonctions constantes, et s'identifie à $\mathbf{k}$, muni de la représentation triviale. Utilisant l'hypothèse $(**)$ pour $C_H\left(\mathrm{Ad}_\rho\right)$ nous obtenons un projecteur H-équivariant de $C_H\left(\mathrm{Ad}_\rho\right)$ sur $\mathbf{k}$. En vertu de l'hypothèse $(**)'$ pour Ad_ρ, tout morphisme H-équivariant $\mathfrak{gl}(V) \to C_H\left(\mathrm{Ad}_\rho\right)$ commute au projecteurs $\pi_{\mathbf{k}}$ et $\pi_{\mathfrak{z}}$ (cf. Remarque *i)*).

Nous nous fixons un tore déployé maximal T de G sur $\mathbf{k}$, notons

$$Y(T) = \mathrm{Hom}(T, GL(1))$$

le groupe des cocaractères et $\Lambda = Y(T) \otimes \mathbf{R}$ l'espace vectoriel réel associé. L'immeuble de Bruhat-Tits de G sur $\mathbf{k}$ est noté $\mathscr{I}(G)$. C'est le quotient de $G(\mathbf{k}) \times \Lambda$ par la relation d'équivalence considérée dans [**RTW09**] (1.3.2) (cf. [**Tit79**], 2.1). Rappelons que G^{an} désigne l'espace analytique associé à G, vu comme espace topologique des semi-normes multiplicatives bornées sur l'algèbre $\mathbf{k}[G]$ des fonctions régulières sur G, pour la topologie de la convergence simple. Nous notons $\theta : \mathscr{I}(G) \to G^{\mathrm{an}}$ une application telle que dans l'énoncé F.3, et nottons G_θ son stabilisateur à droite dans $G(\mathbf{k})$, qui est compact et ouvert.

Nous fixons un point o de $\mathscr{I}(G)$, et notons G_o son stabilisateur dans G_θ. Le groupe G_o est compact dans $G(\mathbf{k})$ ([**Tit79**] 3.2) et Zariski dense dans G ([**RTW09**] Lemma 1.4). Nous notons H_o le groupe compact $G_o \cap H(\mathbf{k})$, et $\mathscr{I}_{\mathbf{k}}(G)^{H_o}$ le lieu fixe de l'action de H_o sur $\mathscr{I}(G)$. D'après le Théorème F.1, nous pouvons choisir un compact C de $\mathscr{I}_{\mathbf{k}}(G)$ tel que $\mathscr{I}_{\mathbf{k}}(G) = Z_G(H)(\mathbf{k}) \cdot C$.

La notion de convexité utilisée est celle introduite dans la section F.

Définition. — Soit alors Y le lieu des points y de $G(\mathbf{k})$ tels que dans l'enveloppe convexe de $H_o \cdot y^{-1} \cdot o$, il se trouve un point de C.

On notera que la construction de Y ne dépend que (de G, de H et) du choix de θ, de o et de C. La partie Y ne dépend donc ni de ρ, ni de Ω. L'énoncé suivant démontre que la partie Y est fermée dans $G(\mathbf{k})$ et satisfait la première condition du Théorème 1.1.

Proposition 2.1. — *La partie Y de $G(\mathbf{k})$ est fermée ; l'intersection $Y \cap Z_G(H)(\mathbf{k})$ est compacte ; on a $G(\mathbf{k}) = Y \cdot Z_G(H)(\mathbf{k})$.*

Démonstration. — Montrons que la partie Y est fermée dans $G(\mathbf{k})$. Par construction, la partie Y est invariante à gauche sous le stabilisateur de o. C'est donc une partie stable sous G_o, qui est ouvert. Le complémentaire de Y est donc ouvert, car stable sous G_o.

Montrons que le saturé $Y \cdot Z_G(H)(\mathbf{k})$ de Y par $Z_G(H)(\mathbf{k})$ vaut $G(\mathbf{k})$. Soit g dans $G(\mathbf{k})$, et formons l'enveloppe convexe $\langle H_o g^{-1} o\rangle$ de $H_o g^{-1} o$ dans $\mathscr{I}_{\mathbf{k}}(G)$. L'action de H_o sur $\langle H_o g^{-1} o\rangle$ a au moins un point fixe, d'après [**Tit79**] 2.3.1. Choisissons-en un, disons p. Comme p est fixe sous H_o, il s'écrit, d'après F.1, sous la forme $z^{-1}\gamma$ avec γ dans C et z dans $Z_G(H)(\mathbf{k})$. Comme l'action de z commute à celle de H_o, nous avons $zH_o g^{-1} o = H_o z g^{-1} o$. Comme l'action de z de $\mathscr{I}_{\mathbf{k}}(G)$ échange les appartement, et est affine sur chaque appartement, nous avons

$$\langle H_o z g^{-1} o\rangle = \langle z H_o g^{-1} o\rangle = z\langle H_o g^{-1} o\rangle.$$

Par conséquent $\langle H_o z g^{-1} o\rangle$ contient le point $zp = z(z^{-1}\gamma) = \gamma$, qui appartient à C. Autrement dit gz^{-1} appartient à Y, ce qu'il nous fallait démontrer.

Montrons que l'intersection $Y \cap Z_G(H)(\mathbf{k})$ est compacte. Tout d'abord c'est un fermé. Comme le stabilisateur G_o de o est compact, et que l'action de $G(\mathbf{k})$ sur $\mathscr{I}_{\mathbf{k}}(G)$ est propre, il suffit de montrer que l'intersection $(Y^{-1} \cdot o) \cap (Z_G(H)(\mathbf{k}) \cdot o)$ est relativement compacte. Or o étant fixe sous G_o, donc sous H_o, l'ensemble $Z_G(H)(\mathbf{k}) \cdot o$ est contenu dans $\mathscr{I}_{\mathbf{k}}(G)^{H_o}$. Mais, par définition, l'intersection de $Y^{-1} \cdot o$ avec $\mathscr{I}_{\mathbf{k}}(G)^{H_o}$ est contennue dans le compact C. □

Ceci étant, il nous reste à démontrer la seconde condition du théorème 1.1, autrement dit à établir la formule (2). Quitte à changer la constante c, la validité de la formule (2) ne dépend de la norme $\|-\|$ qu'à équivalence près. Or, V étant de dimension finie, toutes les normes sont équivalentes (cf. section C.1). Soit B une boule du dual de V. Quitte à appliquer la section C.1, nous pouvons supposer que les hypothèses de la Proposition 2.2 concernant la norme $\|-\|$ sont satisfaites.

Proposition 2.2. — *La situation est celle du Théorème 1.1. Nous utilisons les notations précédentes. En particulier ρ et V sont fixés, et nous avons choisi θ, o et C (de sorte, la partie Y est bien définie).*

Supposons que Ω soit bornée, et que $\|-\|$ soit G_o-invariante, ultramétrique et ne prenne que des valeurs prises par $|-| : \mathbf{k} \to \mathbf{R}$. Alors la formule (2) est satisfaite avec

la constante $c_4/(c_1c_2c_3)$*, où*

$$c_1 = 1 + \sup_{f\in C_G(\mathrm{Ad}_\rho)} \frac{\pi_{\mathbf{k}}(f)}{\sup_{\omega\in\Omega}|f|(\omega)},\ c_2 = \min_{\omega\in\Omega} \left|\!\left|\!\left|\rho(\omega)\right|\!\right|\!\right|^{-1},\ c_3 = \sup_{f\in C_G(\mathrm{Ad}_\rho)} \frac{|f|(\theta(o))}{\sup_{k\in K}|f|(k)}$$

et c_4 *sont obtenues en appliquant les Propositions 3.2, 3.1, 3.5 et 3.9 respectivement.*

3. Propositions

Dans cette section nous réunissons quelques arguments généraux qui serviront à la démonstration de la Proposition 2.2. On pourra passer directement à la section suivante et se reporter aux énoncés ci-dessous au besoin. Les notations sont celles introduites dans la section précédente.

Proposition 3.1. — *Il existe une constante positive inversible* c_2 *telle que pour tout* g *de* $G(\mathbf{k})$ *et tout* v *de* V

$$\sup_{\omega\in\Omega} \left\|\rho(y\cdot\omega)(v)\right\| \geq c_2 \sup_{\omega\in\Omega} \left\|\rho(\omega^{-1}y\cdot\omega)(v)\right\| \tag{3}$$

Démonstration. — Par définition de la norme d'opérateur $\left|\!\left|\!\left|\rho(\omega)\right|\!\right|\!\right|$, pour tous ω, g et v comme dans l'énoncé, nous avons l'inégalité

$$\left\|\rho(\omega^{-1}g\cdot\omega)(v)\right\| \geq \left|\!\left|\!\left|\rho(\omega)\right|\!\right|\!\right|^{-1} \left\|\rho(g\cdot\omega)(v)\right\|. \tag{4}$$

Posons $c_2 = \min_{\omega\in\Omega} \left|\!\left|\!\left|\rho(\omega)\right|\!\right|\!\right|^{-1}$. Comme Ω est non vide et bornée, son image par $\omega \mapsto \left|\!\left|\!\left|\rho(\omega)\right|\!\right|\!\right|^{-1}$ est une partie bornée et non vide de $\mathbf{R}_{>0}$. La constante c_2 est donc positive et inversible, et répond à l'énoncé. □

Proposition 3.2. — *Il existe une constante positive inversible* c_1 *telle que pour tout* f *de* $C_H(\mathrm{Ad}_\rho)$*,*

$$\sup_{\omega\in\Omega}|f(\omega)| \geq \frac{1}{c_1}|\pi_{\mathbf{k}}(f)|. \tag{5}$$

Démonstration. — Comme Ω est borné, l'application $\|-\|_\Omega : f \mapsto \sup_{\omega\in\Omega}|f|(\omega)$ est bien définie sur $C_H(\mathrm{Ad}_\rho)$. C'est manifestement une semi-norme. D'après la condition $(*)$, elle ne s'annule pas : c'est une norme. Comme $C_H(\mathrm{Ad}_\rho)$ est de dimension finie, l'application linéaire $\pi_{\mathbf{k}}$, de $C_H(\mathrm{Ad}_\rho)$ vers $\mathbf{k}$, est bornée, relativement à $\|-\|_\Omega$ et $|-|$. Si $|\!|\!|\pi_{\mathbf{k}}|\!|\!|$ désigne sa norme d'opérateur, alors

$$|\!|\!|\pi_{\mathbf{k}}|\!|\!| \cdot \sup_{\omega\in\Omega}|f(\omega)| \geq |\pi_{\mathbf{k}}(f)|. \tag{6}$$

Par conséquent $c_1 = |\!|\!|\pi_{\mathbf{k}}|\!|\!|$ convient si $|\!|\!|\pi_{\mathbf{k}}|\!|\!| \neq 0$. Si, en revanche, $\pi_{\mathbf{k}} = 0$, alors $c_1 = 1$ convient. Quoiqu'il en soit, $c_1 = 1 + |\!|\!|\pi_{\mathbf{k}}|\!|\!|$ convient toujours. □

Proposition 3.3. — *Pour tout v de V, pour toute forme $\mathbf{k}$-linéaire ϕ dans $V^\vee$ et tout g de $G(\mathbf{k})$,*

$$\omega \mapsto \left(\rho(\omega^{-1}\cdot g\cdot\omega)(v)\middle|\phi\right) \tag{7}$$

définit une fonction sur H (resp. G) appartenant à $C_H\left(\mathrm{Ad}_\rho\right)$ (resp. $C_G\left(\mathrm{Ad}_\rho\right)$).

Démonstration. — Comme $e \mapsto (e(v)|\phi)$ est une forme linéaire sur $\mathfrak{gl}(V)$, l'application (7) est un coefficient matriciel. □

Proposition 3.4. — *Nous utilisons les hypothèses du Théorème 1.1 concernant la représentation ρ. Pour toute forme $\mathbf{k}$-linéaire ϕ de $V^\vee$, la fonction constante sur H*

$$\pi_{\mathbf{R}}\left(\omega \mapsto (\rho(\omega^{-1}\cdot y\cdot\omega)(v)|\phi)\right) \tag{8}$$

vaut

$$\left(\pi_{\mathfrak{z}}(\rho(y))(v)|\phi\right) \tag{9}$$

et, lorsque y varie dans G, définit une fonction régulière sur G appartenant à $C_G\left(\mathrm{Ad}_\rho\right)$ et invariante pour l'action par conjugaison de H sur G.

Démonstration. — La fonction $y \mapsto \left(\pi_{\mathfrak{z}}(\rho(y))(v)|\phi\right)$ est manifestement régulière, et est invariante pour l'action par conjugaison de H sur G, vu que, pour ω dans H,

$$\pi_{\mathfrak{z}}\left(\rho\left(\omega y\omega^{-1}\right)\right) = \rho(\omega)\pi_{\mathfrak{z}}(\rho(y))\rho\left(\omega^{-1}\right) = \pi_{\mathfrak{z}}\left(\rho(y)\right) \tag{10}$$

car $\pi_{\mathfrak{z}}$ est H-équivariant et d'image dans $\mathfrak{z}$.

Pour établir l'égalité de (8) et (9), considérons l'application Φ de $\mathfrak{gl}(V)$ vers $C_H\left(\mathrm{Ad}_\rho\right)$ qui envoie e vers le coefficient matriciel $\omega \mapsto \left(\rho(\omega)e\rho\left(\omega^{-1}\right)(v)\middle|\phi\right)$. C'est une application H-équivariante et, d'après la remarque d., elle commute aux projecteurs $\pi_{\mathfrak{z}}$ et $\pi_{\mathbf{k}}$. Autrement dit

$$\pi_{\mathbf{k}}\left(\omega \mapsto \left(\rho(\omega)e\rho(\omega^{-1})(v)\middle|\phi\right)\right) = \omega \mapsto \left(\rho(\omega)\pi_{\mathfrak{z}}(e)\rho\left(\omega^{-1}\right)(v)\middle|\phi\right).$$

Prenons $e = \rho(y)$. Alors le membre de gauche s'identifie à (8), et, d'après (10), le membre de droite s'identifie à (9). □

Proposition 3.5. — *Pour tout point p de $\mathscr{I}(G)$, l'application $f \mapsto \sup_{k\in K}|f|(k)$ et la restriction de la semi-norme $\theta(p)$ définissent, sur $C_G\left(\mathrm{Ad}_\rho\right)$, deux normes comparables.*

En particulier, il existe une constante positive et inversible c_3 telle que, pour toute fonction f de $C_G\left(\mathrm{Ad}_\rho\right)$, $\sup_{k\in K}|f|(k) \geq \frac{1}{c_3}|f|(\theta(p))$.

Démonstration. — L'existence de c_3 découle de la définition de la comparabilité des normes de la section C.1. D'après la section C.1, il suffit de vérifier que l'on a bien deux normes $(\mathbf{k},|-|)$-homogènes.

L'application $f \mapsto \sup_{k\in K}|f|(k)$ est bien définie car K est compact. C'est manifestement une semi-norme $(\mathbf{k},|-|)$-homogène. Comme K est Zariski dense dans G, cette application ne s'annule en aucune fonction régulière. C'est donc une norme.

Quant à $\theta(p)$, comme il s'agit par définition d'une semi-norme (non nulle, [**Ber90**] 1.1) multiplicative $(\mathbf{k}, |-|)$-homogène sur $\mathbf{k}[G]$, il suffit de vérifier que c'est en fait une norme. Comme $\theta(p)$ est multiplicative, son noyau définit un idéal de $\mathbf{k}[G]$. Comme $\theta(p)$ vaut 1 en 1, c'est idéal est strict. Or le stabilisateur de p dans $G(\mathbf{k})$ est Zariski dense. Cet ideal définit une sous-variété $G(\mathbf{k})$-invariante de G : cette sous-variété ou bien est vide ou bien vaut G lui-même. Or G est réduit, et l'idéal considéré ne contient pas l'unité. Par conséquent cet idéal est nul : $\theta(p)$ ne s'annule pas. □

L'énoncé suivant est un corollaire à la Proposition F.3. La notion de convexité utilisée est celle introduite dans l'appendice correspondant (section F), auquel nous renvoyons. Mentionnons juste que cette notion de convexité est naturellement induite par la structure affine par morceaux standard sur l'immeuble $\mathscr{I}_{\mathbf{k}}(G)$.

Proposition 3.6 **(Convexité)**. — *Pour toute fonction régulière f sur G, l'application $p \mapsto |f|(\theta(p))$ est convexe sur $\mathscr{I}_{\mathbf{k}}(G)$.*

Proposition 3.7 **(Hyperbolicité)**. — *Pour tout point p de $\mathscr{I}_{\mathbf{k}}(G)$ l'enveloppe convexe de $H_o \cdot p$ contient un point fixe de H_o.*

Démonstration. — Notons que comme $\mathscr{I}_{\mathbf{k}}(G)$ est localement réunion finie d'appartements et que $H_o \cdot p$ est compact (C'est l'image du groupe compact H_o par une application continue vers un espace séparé), l'enveloppe convexe de $H_o \cdot p$ est compacte. Il suffit alors d'appliquer [**Tit79**] 2.3.1. et [**BT72**], 3.2.3. □

Proposition 3.8. — *Soit f une fonction convexe sur $\mathscr{I}_{\mathbf{k}}(G)$ et H_o-invariante à gauche sur $Y \cdot o$, et un point p appartenant à $Y \cdot o$. Alors*

$$f(p) \geq \min_{\gamma \in C} f(\gamma). \tag{11}$$

Démonstration. — Comme f est H_o-invariante sur $Y \cdot o$, nous avons $f(p) = \max_{x \in H_o \cdot p} f(x)$. Notons $\langle H_o \cdot p \rangle$ l'enveloppe convexe de $H_o \cdot p$. Comme f est convexe, $\max_{x \in H_o \cdot p} f(x) = \max_{x \in \langle H_o \cdot p \rangle} f(x)$. Lorsque p appartient à $Y \cdot o$, $C \cap \langle H_o \cdot p \rangle$ est non vide. D'où

$$f(p) = \max_{x \in \langle H_o \cdot p \rangle} f(x) \geq \max_{x \in \langle H_o \cdot p \rangle \cap C} f(x) \geq \min_{x \in \langle H_o \cdot p \rangle \cap C} f(x) \geq \min_{\gamma \in C} f(\gamma).$$

□

Dans la proposition suivante, C désigne le compact de $\mathscr{I}_{\mathbf{k}}(G)$ défini dans la section précédente, et B la boule unité du dual de V.

Dans cette proposition, on étudie les coefficients matriciels de la forme $g \mapsto \phi(\pi_\lambda(\rho(g))(v))$ comme fonction sur G^{an}, et en particulier sur l'image de C dans G^{an} par l'application $\theta : \mathscr{I}_{\mathbf{k}}(G) \to G^{\mathrm{an}}$. On notera donc

$$|\phi|(\pi_\lambda(\rho(\theta(\gamma)))(v))$$

la valeur obtenue en appliquant, pour γ dans C la norme $\theta(\gamma)$ au coefficient matriciel $g \mapsto \phi(\pi_\mathfrak{z}(\rho(g))(v))$. Pour alléger les notations, on pourra omettre θ et ρ dans les notations, soit

$$|\phi|(\pi_\mathfrak{z}(\gamma)(v)) := |\phi|(\pi_\mathfrak{z}(\rho(\theta(\gamma)))(v)).$$

Proposition 3.9. — *Il existe une constante c_4 telle que pour tout élément γ de C, et tout élément v de V,*

$$\sup_{\phi\in B}(|\phi|\pi_\mathfrak{z}(\gamma))(v) \geq \|v\|/c_4, \tag{12}$$

Démonstration. — Remarquons tout d'abord que, d'après la proposition 3.5, la semi-norme $\theta(\gamma)$ est une norme, pour tout γ dans C.

La restriction de la norme $\theta(\gamma)$ à $C_G\left(\mathrm{Ad}_\rho\right)$ dépend continûment de γ, pour la topologie faible. Comme $C_G\left(\mathrm{Ad}_\rho\right)$ est de dimension finie et C est compact, ces normes sont « uniformément équivalentes » pour γ dans C : il existe une constante c' telle que pour tous γ et γ' dans C nous ayons $\forall f \in C_G\left(\mathrm{Ad}_\rho\right), |f|(\theta(\gamma)) \geq c'|f|(\theta(\gamma'))$. Il suffira de vérifier la formule (12) pour une constante c_4' et *pour un seul γ de C* : la constante $c_4 = c'c_4'$ conviendra alors pour tout γ dans C.

Fixons γ dans C. La formule est évidente pour $v = 0$. Nous pouvons donc supposer que $v \neq 0$, et même, par homogénéité, que, pour une certaine constante c'' ne dépendant que de $\|-\|$, le vecteur v appartienne au compact $V_{c''}$ où l'inégalité $1/c'' \leq \|v\| \leq c''$ est satisfaite.

Tout revient ainsi à montrer que

$$\inf_{v\in V_{c''}} \sup_{\phi\in B}|\phi|(\pi_\mathfrak{z}(\gamma)(v)) > 0.$$

Soit par l'absurde une suite $(v_n)_{n\in\mathbf{N}}$ de $V_{c''}$ telle que

$$\lim_{n\in\mathbf{N}} \sup_{\phi\in B}|\phi|(\pi_\mathfrak{z}(\gamma)(v_n)) = 0.$$

Comme $V_{c''}$ est compact et n'adhére pas à 0, la suite $(v_n)_{n\in\mathbf{N}}$ a une valeur d'adhérence non nulle v_∞. Nous allons montrer, ce qui sera une contradiction, que v_∞ est nécessairement nul.

Pour tout ϕ_0 dans B, on conclut de l'encadrement

$$0 \leq |\phi_0|(\pi_\mathfrak{z}(\gamma)(v_n)) \leq \sup_{\phi\in B}|\phi|(\pi_\mathfrak{z}(\gamma)(v_n)) = 0$$

que $\lim_{n\in\mathbf{N}}|\phi_0|(\pi_\mathfrak{z}(\gamma)(v_n)) = 0$. Par continuité de $v \mapsto |\phi_0|(\pi_\mathfrak{z}(\gamma)(v)$, il s'ensuit que $|\phi_0|(\pi_\mathfrak{z}(\gamma)(v_\infty) = 0$.

Ainsi, pour tout ϕ de B, $|\phi|(\pi_\mathfrak{z}(\gamma)(v_\infty)) = 0$. Autrement dit, comme $\theta(\gamma)$ est une norme, chaque coefficient matriciel $g \mapsto \phi(\pi_\mathfrak{z}(\rho(g))(v_\infty))$ est identiquement nul. Par conséquent, pour tout g dans $G(\mathbf{k})$, le vecteur $\pi_\mathfrak{z}(\rho(g))(v_\infty)$ est nul. Mais, lorsque g vaut l'élément neutre,

$$\pi_\mathfrak{z}(\rho(g))(v_\infty) = \pi_\mathfrak{z}(\mathrm{Id}_V)(v_\infty) = \mathrm{Id}_V(v_\infty) = v_\infty \neq 0.$$

□

4. Démonstration

Démontrons la Proposition 2.2. Nous utilisons les notations de la section 2, et les arguments de la section 3.

Démonstration. — Comme $\|-\|$ est supposée G_o-invariante, nous pouvons substituer $\sup_{k\in G_o}\left\|\rho(k\cdot y\cdot\omega)(v)\right\|$ à $\left\|\rho(y\cdot\omega)(v)\right\|$ dans la formule (2), ce qui donne

$$\forall y\in Y,\forall v\in V,\sup_{\omega\in\Omega}\sup_{k\in G_o}\left\|\rho(k\cdot y\cdot\omega)(v)\right\|\geq\|v\|/c. \tag{13}$$

D'après la proposition 3.1, il suffit d'établir

$$\forall y\in Y,\forall v\in V,\sup_{\omega\in\Omega}\sup_{k\in G_o}\left\|\rho\left(\omega^{-1}\cdot k\cdot y\cdot\omega\right)(v)\right\|\geq\frac{1}{c\cdot c_2}\cdot\|v\|. \tag{14}$$

Soit $V^\vee$ le dual algébrique de V, et notons B sa boule unité. D'après la section C.1 et les hypothèses sur $\|-\|$, nous avons $\|v\|=\sup_{\phi\in B}|\phi(v)|$. La formule qui précède équivaut donc à la suivante.

$$\forall y\in Y,\forall v\in V,\sup_{\omega\in\Omega}\sup_{\phi\in B}\sup_{k\in G_o}|\phi|\left(\rho\left(\omega^{-1}\cdot k\cdot y\cdot\omega\right)(v)\right)\geq\frac{1}{c\cdot c_2}\|v\|. \tag{15}$$

D'après 3.3, la fonction $\omega\mapsto\phi\left(\rho\left(\omega^{-1}\cdot k\cdot y\cdot\omega\right)(v)\right)$ sur H appartient à $C_H\left(\mathrm{Ad}_\rho\right)$. Appliquant la proposition 3.2, il sort

$$\sup_{\omega\in\Omega}|\phi|\left(\rho\left(\omega^{-1}\cdot k\cdot y\cdot\omega\right)(v)\right)\geq\frac{1}{c_1}\left|\pi_{\mathbf{k}}\left(\omega\mapsto\phi\left(\rho\left(\omega^{-1}\cdot k\cdot y\cdot\omega\right)(v)\right)\right)\right|. \tag{16}$$

D'après 3.4, le membre de droite de (16) de vaut

$$\frac{1}{c_1}|\phi|(\pi_\mathfrak{z}(ky)(v)). \tag{17}$$

D'après 3.5, il existe une constante positive et inversible c_3 telle que

$$\sup_{k\in G_o}|\phi|(\pi_\mathfrak{z}(ky)(v))\geq\frac{1}{c_3}|\phi|(\pi_\mathfrak{z}(oy)(v)). \tag{18}$$

Par conséquent, nous avons établi (combinant (16), (17) et (18))

$$\forall y\in Y,\forall v\in V,\sup_{\omega\in\Omega}\sup_{k\in G_o}|\phi|\left(\rho\left(\omega^{-1}\cdot k\cdot y\cdot\omega\right)(v)\right)\geq\frac{1}{c_1\cdot c_3}|\phi|(\pi_\mathfrak{z}(oy)(v)),$$

d'où, en considérant la borne supérieure relative aux ϕ dans B,

$$\forall y\in Y,\forall v\in V,\sup_{\omega\in\Omega}\sup_{\phi\in B}\sup_{k\in G_o}|\phi|\left(\rho\left(\omega^{-1}\cdot k\cdot y\cdot\omega\right)(v)\right)\geq\frac{1}{c_1\cdot c_3}\sup_{\phi\in B}|\phi|(\pi_\mathfrak{z}(oy)(v)), \tag{19}$$

Ainsi, pour démontrer (15), il suffit d'établir

$$\frac{1}{c_1 \cdot c_3} \sup_{\phi \in B} |\phi|(\pi_\mathfrak{z}(oy)(v)) \geq \|v\| \frac{1}{c \cdot c_2}. \tag{20}$$

D'après la proposition 3.4 la fonction $g \mapsto \phi(\pi_\mathfrak{z}(g)(v))$ est régulière sur G en la variable g, et invariante sous l'action de H par conjugaison. Or, pour h dans H_o et $y^{-1} \cdot o$ dans $Y^{-1} \cdot o$, nous avons

$$h\theta(y^{-1}o)h^{-1} = h\theta(y^{-1}o)$$

car G_θ contient h^{-1}, et

$$h\theta(y^{-1}o) = \theta(hy^{-1}o)$$

car θ est équivariante. Sur $Y^{-1} \cdot o$, la fonction $y^{-1}o \mapsto |\phi|(\pi_\mathfrak{z}(\theta(y^{-1}o))(v))$ est donc invariante à gauche sous H_o.

D'après la Proposition 3.6 la fonction $p \mapsto |\phi|(\pi_\mathfrak{z}(\theta(p))(v))$ est convexe sur $\mathscr{I}_\mathbf{k}(G)$. Par conséquent la fonction $g \mapsto \sup_{\phi \in B} |\phi|(\pi_\mathfrak{z}(g)(v))$ est convexe sur $\mathscr{I}_\mathbf{k}(G)$ et sa restriction à $Y^{-1} \cdot o$ est invariante à gauche sous H_o. D'après la Proposition 3.8, on a, pour tout y de Y,

$$\sup_{\phi \in B} |\phi|(\pi_\mathfrak{z}(y^{-1}o)(v)) \geq \inf_{\gamma \in C} \sup_{\phi \in B} |\phi|(\pi_\mathfrak{z}(\gamma)(v)).$$

Or, d'après la Proposition 3.9, nous avons

$$\forall v \in V, \forall \gamma \in C, \sup_{\phi \in B} |\phi|(\pi_\mathfrak{z}(\gamma)(v)) \geq \|v\| / c_4.$$

Ce qui démontre bien la formule (20), avec la constante $c = \frac{c_1 c_3 c_4}{c_2}$. □

ANNEXE

Dans cet annexe, nous faisons quelques rappels sur les groupes algébriques, les espaces analytiques et les immeubles. Nous y démontrons notamment (Théorème F.1) un résultat de décomposition sur les immeubles et (Théorème F.3) un résultat sur la convexité logarithmique des fonctions régulières sur l'immeuble, une fois plongé dans l'espace analytique.

Algèbre. — Dans cette partie, les unités sont supposées non nulles, et les seuls algèbres, anneaux et corps à considérer seront associatifs, commutatifs et unifères. (Dans la seconde partie interviendront en revanche des algèbres de Lie). On se fixe un corps de base $\mathbf{k}$. Nous notons $\mathbf{Alg}_\mathbf{k}$ la catégorie des $\mathbf{k}$-algèbres commutatives et unifères *de type fini*.Nous fixerons également, par commodité, une extension algébrique séparable maximale $\mathbf{k}_s$ (c.-à-d. séparable close) de $\mathbf{k}$.

Appendice A
Variétés algébriques affines

A.1. Définition. — On appelle *variété algébrique affine* sur un corps $\mathbf{k}$ les *schémas affines* non vides de [**Gro60**] 1.7.1 qui, suivant [**Gro60**] 6.4.1, sont des $\mathbf{k}$-*schémas algébriques*. Concrètement ce sont les espaces annelés $(X,\mathscr{O}_X)$ non vides isomorphes au spectre premier $\mathrm{Spec}(A)$ (cf. [**Gro60**] 1.1.1) d'une $\mathbf{k}$-algèbre A de $\mathbf{Alg}_{\mathbf{k}}$, muni de la topologie de Zariski (topologie *spectrale* au sens de [**Gro60**] 1.1.1), et de son faisceau structural $\widetilde{A}$ (cf. [**Gro60**] 1.3.4), vu comme faisceau de $\mathbf{k}$-algèbres (cf. [**Gro60**] 2.5.1). En particulier toute algèbre A de $\mathbf{Alg}_{\mathbf{k}}$ définit canoniquement une variété algébrique affine. L'opération inverse qui, partant d'une variété algébrique affine $(X,\mathscr{O}_X)$ sur $\mathbf{k}$, lui associe la $\mathbf{k}$-algèbre $\mathscr{O}_X(X)$ des sections globales de son faisceau $\mathscr{O}_X$ de $\mathbf{k}$-algèbres fournit une antiéquivalence réciproque entre la catégorie $\mathbf{Aff}_{\mathbf{k}}$ des variétés algébriques affines sur $\mathbf{k}$ et $\mathbf{Alg}_{\mathbf{k}}$.

A.2. Fonctions régulières, coordonnées, sous-variétés fermées. — Par exemple, pour tout entier naturel N, le schéma $\mathbf{A}^N_{\mathbf{k}} = (\mathrm{Spec}(A), \widetilde{A})$ associé à l'algèbre de polynômes $\mathbf{k}[T_1,\dots,T_N]$ est une variété algébrique affine, que l'on appellera *espace affine de dimension N sur $\mathbf{k}$*. Tout idéal strict I de $\mathbf{k}[T_1,\dots,T_N]$ permet de définir le morphisme quotient $\mathbf{k}[T_1,\dots,T_N] \to \mathbf{k}[T_1,\dots,T_N]/I$, d'où, par antiéquivalence, un morphisme de variété algébriques $Z(I) \to \mathbf{A}^N_{\mathbf{k}}$. On dit que $Z(I)$ est un *sous-schéma fermé de* $\mathbf{A}^N_{\mathbf{k}}$. On appelle sous-schéma fermé (non vide) de $Z(I)$ une variété de la forme $Z(J)$, où J est idéal strict contenant I. Une sous-schéma fermé de $Z(I)$ sera implicitement muni du morphisme $Z(J) \to Z(I)$ correspondant au morphisme d'algèbres $\mathbf{k}[T_1,\dots,T_N]/I \to \mathbf{k}[T_1,\dots,T_N]/J$.

Notons $\mathbf{k}[V]$ la $\mathbf{k}$-algèbre $\mathscr{O}_X(X)$ associée à une variété algébrique affine $V = (X,\mathscr{O}_X)$. Une *fonction régulière* sur V désigne un élément de l'algèbre associée $k[V]$. Nous appellerons *système de coordonnées sur V* le choix d'une famille finie $(f_1,\dots,f_n)$ de fonctions régulières engendrant l'algèbre $\mathbf{k}[V]$.

Ce choix permet d'identifier une variété algébrique avec un sous-schéma fermé $Z(I)$ de l'espace affine $\mathbf{A}^n_{\mathbf{k}}$: celui défini par l'idéal I de $\mathbf{k}[T_1,\dots,T_N]$ des polynômes dont l'évaluation en $(f_1,\dots,f_n)$ est l'élément nul de l'algèbre $\mathbf{k}[V]$. Cela correspond, par antiéquivalence, à l'isomorphisme $\mathbf{k}[T_1,\dots,T_N]/I \to \mathbf{k}[V]$ qui envoie T_i sur f_i. Cette construction justifie *a posteriori* le qualificatif « affine » pour les variétés algébriques considérées (et par extension pour les schémas affines de [**Gro60**]).

Ayant implicitement choisi un système de coordonnées sur V et identifié V à $Z(I)$, on appellera *sous-variété fermée* de V un sous-schéma fermé $Z(J)$ de $Z(I)$, le choix d'un morphisme $Z(J) \to Z(I) = V$ étant lui aussi implicite.

A.3. Foncteurs des points. — Remarquons qu'un morphisme d'une variété algébrique affine W, d'algèbre A, dans la variété algébrique affine V, munie du

système de coordonnées $(f_1,\dots,f_n)$ revient, par antiéquivalence, à choisir une famille $(a_1,\dots,a_n)$ image de $(f_1,\dots,f_n)$ dans A^n, cette famille devant satisfaire toutes les équations polynomiales à coefficient dans $\mathbf{k}$ satisfaites dans $\mathbf{k}[V]$ par le système de coordonnées $(f_1,\dots,f_n)$. Nous dirons que la famille $(a_1,\dots,a_n)$ est un *point* de V *à coordonnées dans* A, et que les éléments a_i sont ses coordonnées. On note $V(A)$ l'ensemble des points de V à coordonnées dans A.

Étant donné un morphisme de $\mathbf{k}$-algèbres de type fini $\phi : A \to A'$, on obtient une application $V(\phi) : V(A) \to V(A')$ en envoyant un point $(a_1,\dots,a_n)$ sur le point $(\phi(a_1),\dots,\phi(a_n))$. Il est immédiat que V définit ainsi un foncteur covariant de la catégorie $\mathbf{Alg}_{\mathbf{k}}$ des $\mathbf{k}$-algèbres commutatives unifères de type fini vers celle des ensembles. Nous dirons que ce foncteur est le *foncteur des points* de V.

Étant donné un morphisme $\Phi : V \to V'$ de variétés algébriques affines, munies de systèmes de coordonnées $(f_1,\dots,f_n)$ et $(g_1,\dots,g_m)$, on obtient, en composant tout morphisme $W \to V$ par Φ, une application $V(A) \to V'(A)$. Ces applications, lorsque A, varie s'inscrivent dans une transformation naturelle entre les foncteurs des points associés à V et V'.

En vertu du lemme de Yoneda, V est déterminé par son foncteur des points, à isomorphisme près. Plus précisément, les morphismes entre V et V' correspondent biunivoquement aux transformations naturelles entre foncteurs des points.

A.4. Variétés réduites, point de vue de Weil. — Rappelons que $\mathbf{k}_s$ désigne une extension algébrique séparable et séparablement close de $\mathbf{k}$.

Si l'algèbre $\mathbf{k}[V]$ est *réduite*, c'est à dire sans élément nilpotent, on dit que la variété V est *réduite*. La variété $Z(I)$ n'est réduite que si l'idéal strict I est radiciel, c'est à dire stable dans $\mathbf{k}[T_1,\dots,T_N]$ par formation de racines d'ordre quelconque (appartenant à $\mathbf{k}[T_1,\dots,T_N]$).

Dans ce cas $Z(I)$ et $\mathbf{k}$ sont déterminés par la connaissance de l'ensemble $Z(I)(\mathbf{k}_s)$ des points à coordonnées dans $\mathbf{k}_s$ muni de l'action de $\mathrm{Aut}(\mathbf{k}_s/\mathbf{k})$ sur les coordonnées : $\mathbf{k}$ est le corps fixe de $\mathrm{Aut}(\mathbf{k}_s/\mathbf{k})$ agissant sur $\mathbf{k}_s$, et l'idéal I est formé des polynômes à coefficients dans $\mathbf{k}$ qui s'annulent sur $Z(I)(\mathbf{k}_s)$. Le premier point découle de la correspondance de Galois, et le dernier point est une formulation du *Nullstellensatz* de D. Hilbert.

En outre, le corps k_s étant nécessairement infini, on peut en déduire, que les application $\Phi : V \to W$ entre variétés réduites correspondent aux applications $V(\mathbf{k}_s) \to W(\mathbf{k}_s)$ qui sont des applications polynomiales (relativement au système de coordonnées choisis sur V et W). En fait il n'est pas nécessaire de supposer que W soit réduite.

On dit que V est *géométriquement réduite* si, pour une extension algébriquement close $\bar{\mathbf{k}}$ de $\mathbf{k}$, la variété algébrique affine sur $\bar{\mathbf{k}}$ associée à l'algèbre $\mathbf{k}[V] \otimes_{\mathbf{k}} \bar{\mathbf{k}}$ est réduite.

Appendice B

Groupes algébriques affines, linéaires, réductifs

B.1. Groupes algébriques affines. — Un *groupe algébrique affine* sur un corps $\mathbf{k}$ désigne un objet en groupes dans la catégorie des variété algébriques affines sur $\mathbf{k}$. Il revient au même de se donner une variété algébrique affine G sur $\mathbf{k}$ et une structure de $\mathbf{k}$-algèbre de Hopf sur $\mathbf{k}[G]$. Étant donné un système de coordonnées sur G, il est encore équivalent, en vertu du lemme de Yoneda, de se donner, pour toute algèbre A de $\mathbf{Alg}_\mathbf{k}$ une structure de groupe sur $G(A)$ dont la loi de groupe est la restriction à $G(A)$ d'une application polynomiale, ces structures de groupes étant telles que pour tout morphisme $A \to A'$ dans $\mathbf{Alg}_\mathbf{k}$, l'application $G(A) \to G(A')$ soit un homomorphisme de groupes.

Un groupe algébrique affine est dit *réduit* lorsque la variété sous-jacente est réduite. Pour une variété algébrique affine réduite G, se donner une structure de groupe algébrique affine G revient à se donner une loi de groupe sur $G(\mathbf{k}_s)$ qui soit une application polynomiale à coefficients dans $\mathbf{k}$ (relativement au système de coordonnées choisi). Le groupe $\mathrm{Aut}(\mathbf{k}_s/\mathbf{k})$ agit alors par automorphismes de groupes sur $G(\mathbf{k}_s)$.

Un *morphisme* de groupes algébriques affines est un morphisme d'objets en groupes, c'est-à-dire un morphisme de variétés algébrique affines compatible à la loi de groupe.

B.2. Représentations linéaires. — Soit V un espace vectoriel de dimension finie sur $\mathbf{k}$. Alors le foncteur $V_\mathbf{k} : A \mapsto V \otimes A$ sur $\mathbf{Alg}_\mathbf{k}$ est isomorphe au foncteur des points de l'espace affine de dimension $\dim_\mathbf{k}(V)$. Il suffit en effet de choisir une base de V sur $\mathbf{k}$ pour construire un tel isomorphisme. De même, quitte à choisir une base de $\mathbf{k}$-espace vectoriel de $\mathrm{End}_\mathbf{k}(V)$, on identifie le foncteur analogue $\mathrm{End}(V)_\mathbf{k} : A \mapsto \mathrm{End}(V \otimes A)$ au foncteur des points d'une variété algébrique affine, l'espace affine de dimension $\dim(V)^2$. Le foncteur $GL(V)_\mathbf{k} : A \mapsto GL(V \otimes A)$ est naturellement muni d'une structure de foncteur en groupes. Pour identifier ce foncteur au foncteur de points d'une variété algébrique, on pourra choisir le plongement $GL(V \otimes A) \to A \times \mathrm{End}_A(V \otimes (A))$ dont le premier facteur est l'inverse de l'application déterminant (en base A), et le second l'inclusion naturelle. Ce plongement identifie $GL(V \otimes A)$ avec le lieu des couples (d, M) tels que $d \cdot \det(M) = 1$. Quitte à choisir une base de $\mathbf{k} \times \mathrm{End}_\mathbf{k}(V)$, on identifie le foncteur $GL(V)_\mathbf{k}$ au foncteur des points d'une variété. Il s'agit en fait d'un groupe algébrique *réduit*.

On appellera *représentation linéaire* d'un groupe algébrique affine G sur V un morphisme de foncteurs en groupes du foncteur des points de G vers $GL(V)_\mathbf{k}$. Si l'on identifie $GL(V)_\mathbf{k}$ à un groupe algébrique affine, cela revient à un morphisme de groupe algébriques affines de G dans $GL(V)_\mathbf{k}$. Il revient encore au même de

se choisir pour tout A dan $\mathbf{Alg}_{\mathbf{k}}$ une action de $G(A)$ sur $V \otimes A$, cette action étant compatible aux morphismes dans $\mathbf{Alg}_{\mathbf{k}}$.

Lorsque G est réduit, il revient au même de se donner une représentation $\mathbf{k}_s$-linéaire $\mathrm{Aut}(\mathbf{k}_s/\mathbf{k})$-équivariante $G(\mathbf{k}_s) \to GL(V \otimes \mathbf{k}_s)$ qui soit une application polynomiale.

B.3. Tores déployés. — Par exemple, lorsque V est de dimension 1, et que l'on fixe un isomorphisme $T : V \to \mathbf{A}^1_{\mathbf{k}}$, le foncteur $GL(V)_{\mathbf{k}}$ s'identifie d'une part au foncteur *groupe multiplicatif* $\mathbf{G_m} : A \mapsto A^\times$, (où $\mathbf{G_m}(A)$ agit sur $V \otimes A$ par homothéties) et au foncteur associé à la variété algébrique d'algèbre $\mathbf{k}[T, T^{-1}]$.

Plus généralement, pour tout entier naturel n, le foncteur groupe linéaire $GL(n)_{\mathbf{k}} : A \mapsto GL(n, A)$ s'identifie naturellement au foncteur $GL(V)_{\mathbf{k}}$, pour $V = \mathbf{k}^n$, et peut donc s'identifier à un groupe algébrique affine. Lorsque $n = 1$, alors $GL(1)$ s'identifie à $\mathbf{G_m}$.

On définit le produit de groupe algébriques affines en effectuant le produit des foncteurs en groupes correspondants. Un tore déployé désigne un groupe algébrique affine (dont le foncteur des points est) isomorphe à un produit de copies de $GL(1)$, vu comme groupe algébrique affine.

Pour un tore déployé T, on appelle *caractère* de T un morphisme de groupes algébriques affines de T dans $GL(1)$. Tout caractère induit un morphisme de T vers l'espace affine de dimension 1, et par antiéquivalence une fonction régulière sur T. Par produit dans $GL(1)$, les caractères forment un groupe abélien, que l'on notera $X(T)$. Il s'agit aussi du produit des fonctions régulières correspondantes. En le vérifiant dans le cas $T = GL(1)^n$, on montre que $X(T)$ est un groupe est un groupe abélien libre de rang fini, et que $X(T)$ est une base de l'algèbre $\mathbf{k}[T]$ comme espace vectoriel sur $\mathbf{k}$. Ainsi on pourra identifier $\mathbf{k}[T]$ avec l'algèbre de groupe $\mathbf{k}[X(T)]$.

B.4. Sous-groupes algébriques. — Un *sous-groupe algébrique* d'un groupe algébrique G affine désignera une sous-variété fermée V de G telle que pour tout A dans $\mathbf{Alg}_{\mathbf{k}}$, $V(A)$ soit un sous-groupe de $G(A)$, la sous-variété V étant alors munie de la structure de groupe algébrique affine correspondante.

Étant donné un sous-groupe algébrique H de G, on définit son centralisateur comme le plus grand sous-groupe fermé Z tel que pour tout A dans $\mathbf{Alg}_{\mathbf{k}}$, $Z(A)$ et $H(A)$ commutent dans $G(A)$. De manière équivalente, il s'agit du sous-groupe fermé associé au sous-foncteur $A \mapsto Z(A)$ de $A \mapsto G(A)$ qui envoie A sur le sous-groupe de $G(A)$ formé des éléments g qui commutent à $H(A)$ et dont l'image dans $G(B)$ commute à $H(B)$ pour toute algèbre B contenant A.

Lorsque H vaut G, on définit ainsi le centre de G.

Lorsque H est réduit, bien que le centralisateur $Z_H(G)$ de H dans G ne soit pas nécessairement réduit, le groupe $Z_G(H)(\mathbf{k}_s)$ est le centralisateur de $H(\mathbf{k}_s)$ dans $G(\mathbf{k}_s)$.

B.5. Groupes algébriques réductifs, semi-simples. — Suivant [**BT65**] 0.7, on appelle *groupe réductif* un groupe algébrique affine *géométriquement réduit* (cf. [**BT65**], 0.3) dont le « *radical unipotent* » est nul. Cela signifie aussi que tout sous-groupe algébrique connexe *géométriquement réduit*, résoluble et distingué est central.

Un *groupe algébrique semi-simple* est un groupe réductif G dont le centre Z est *fini*, au sens où $Z(\mathbf{k}_s)$ est fini, ou, de manière équivalente, $\mathbf{k}[Z]$ est de dimension finie sur $\mathbf{k}$.

Appendice C

Corps locaux ultramétriques

Considérons un *corps local* $\mathbf{k}$, c'est-à-dire un corps topologique commutatif localement compact et non discret. Munissons le d'une *valeur absolue* $|-|$, c'est-à-dire une application de $\mathbf{k}$ vers $\mathbf{R}$ dont la restriction à $\mathbf{k}^\times$ définit un morphisme multiplicatif $\mathbf{k}^\times \to \mathbf{R}^\times$ et telle que $(x,y) \mapsto |x-y|$ définisse une distance compatible à la topologie. On pourra par exemple prendre comme valeur absolue le *module* de $\mathbf{k}$ ([**Bou63**] §10).

Supposons cette valeur absolue *ultramétrique*, c'est-à-dire que l'inégalité triangulaire est renforcée par la propriété

$$\forall x, y \in \mathbf{k}, |x+y| \leq \max\{|x|;|y|\}. \tag{21}$$

De manière équivalente, tout point d'une boule en est un centre. En particulier les boules fermées sont aussi des ouverts.

Il en résulte que la boule unité fermée définit un anneau local complet et compact $\mathscr{O}_\mathbf{k}$ dont l'idéal maximal $\mathfrak{m}_\mathbf{k}$ est donné par la boule unité ouverte. Son corps résiduel $\widetilde{\mathbf{k}} = \mathscr{O}_\mathbf{k}/\mathfrak{m}_\mathbf{k}$ est compact et discret, donc fini. Soit p la caractéristique ce corps. Alors $\mathbf{k}$ est isomorphe à une extension finie de $\mathbf{Q}_p$ ou de $\mathbf{F}_p((T))$; l'anneau $\mathscr{O}_\mathbf{k}$ correspond alors à la fermeture intégrale de $\mathbf{Z}_p$ ou $\mathbf{F}_p[[T]]$ respectivement. L'anneau $\mathscr{O}_\mathbf{k}$ est principal, et un générateur ϖ de l'idéal $\mathfrak{m}_\mathbf{k}$ s'appelle une *uniformisante*. Dans le cas des extensions de $\mathbf{F}_p((T))$ les uniformisantes sont les coordonnées formelles.

La valeur absolue et la topologie sur $\mathbf{k}$ proviennent d'une valuation discrète sur cet l'anneau $\mathscr{O}_\mathbf{k}$ (cf. [**Ser68**], I §1,II §1). La valeur absolue sur $\mathbf{k}$ est déterminée par sa valeur en une uniformisante, ou plus généralement en tout élément non nul situé hors de la sphère unité (et la connaissance de l'élément où cette valeur est prise). Il s'ensuit que pour toute extension finie $\mathbf{k}'$ de $\mathbf{k}$, qui est un corps local pour sa topologie en tant qu'espace vectoriel de dimension finie sur $\mathbf{k}$, chaque valeur absolue sur $\mathbf{k}$ s'étend de manière unique en une valeur absolue sur $\mathbf{k}'$.

À isomorphisme près, il n'existe que deux corps locaux n'admettant pas de valeur absolue ultramétrique. Il s'agit de $\mathbf{R}$ et $\mathbf{C}$, qui sont archimédiens.

C.1. Espaces vectoriels normés. — Tout espace vectoriel V de dimension finie sur $\mathbf{k}$ admet une base, ce qui permet de définir la topologie produit relative à une base. On vérifie directement qu'un endomorphisme linéaire de V est continu. Ainsi, les automorphismes linéaires sont donc des homeomorphismes pour cette topologie, qui ne depend donc pas de la base choisie.

Nous appelerons *norme* sur V une application $\|-\| : V \to \mathbf{R}$ telle que l'application $(x,y) \mapsto \|x-y\|$ définisse une distance compatible à la topologie. Cette norme est dite $(\mathbf{k},|-|)$-*homogène*, ou plus simplement *homogène*, lorsque toute homothétie de rapport λ agit sur les distances d'un facteur $|\lambda|$:

(22) pour tout λ dans $\mathbf{k}$ et v dans V, nous avons $\|\lambda \cdot v\| = |\lambda| \cdot \|v\|$.

Nous dirons que deux normes $\|-\|$ et $\|-\|'$ sont *comparables* s'il existe une constante positive et inversible C telle que pour tout v dans V, nous ayons $\|v\| \leq C\|v\|'$ et $\|v\|' \leq C\|v\|$. Remarquons qu'avec notre définition, étant donné une norme $\|-\|$, son carré définit une norme $\|-\|$ qui ne lui est pas comparable. Montrons, qu'en revanche, deux normes *homogènes* sont toujours comparables.

Démonstration. — Soient $\|-\|$ et $\|-\|'$ deux normes homogènes. Quitte à échanger les rôles il suffit de trouver une constante C positive et inversible C telle que $\|-\| \leq C\|-\|'$.

Comme $\mathbf{k}$ n'est pas discret, $\{0\}$ est dans l'adhérence de $\mathbf{k}^\times$. Or lorsque λ tend vers 0 dans $\mathbf{k}$, $\lambda \cdot v$ tend vers l'origine de V. Cela se vérifie coordonnée par coordonnée dans une base de V. Ainsi pour tout v de V, $\mathbf{k}^\times \cdot v$ adhère en l'origine. Ainsi pour toute boule ouverte de V (centrée en l'origine), son orbite sous $\mathbf{k}^\times$ recouvre V.

Par homogénéité, il suffit donc de vérifier l'inégalité $\|-\| \leq \|-\|'$ sur la boule unité fermée B de $\|-\|'$. Soit λ un élément non nul dans l'idéal maximal $\mathfrak{m}_{\mathbf{k}}$, de sorte que $0 < |\lambda| < 1$. Alors par homogénéité on peut également supposer que v n'appartient pas à la boule $\lambda \cdot B$.

Or V, en tant que produit fini d'espace localement compacts, est lui aussi localement compact. Il en résulte que toute boule centrée suffisamment petite est un voisinage relativement compacte de l'origine. □

Étant donné une norme sur V, son dual algébrique acquiert une norme duale : à toute forme $\mathbf{k}$-linéaire sur V on associe sa norme en tant qu'application linéaire de V vers $\mathbf{k}$. Autrement dit on pose $\|\phi\| = |||\phi||| = \sup_{\|v\|\leq 1} \|\phi(v)\|$.

On dit que la norme $\|-\|$ est *ultramétrique* si

(23) $$\forall x, y \in V, \|x+y\| \leq \max\{\|x\|; \|y\|\}.$$

Lemme C.1. — *Soit V un espace vectoriel normé de dimension finie sur* $\mathbf{k}$*, et doit B la boule unité de son dual. Alors on a l'inégalité*

$$\forall v \in V, \|v\| \geq \sup_{b\in B} |\phi(v)|,$$

et il n'y a égalité, simultanément pour tout v de V, que si et seulement si $\|-\|$ est ultramétrique et si les valeurs, dans $\mathbf{R}$*, prises par $\|-\|$ sont celles prises par $|-|$.*

Démonstration. — L'inégalité résulte de ce que pour tout ϕ dans B, nous avons $\|\|\phi\|\| \leq 1$ et de ce que, par définition de la norme triple $\|\phi(v)\| \leq \|\|\phi\|\| \, \|v\|$.

Le sens direct de l'équivalence découle de [**Wei74**], II §1, Prop. 4 (p. 26).

Dans le sens réciproque, on vérifie directement que le membre de droite est une norme ultramétrique et ne prend que des valeurs prises par $|-|$.

□

C.2. Topologies ultramétriques. — Pour toute variété algébrique affine V sur $\mathbf{k}$, et tout système de coordonnées sur V l'inclusion de $V(\mathbf{k})$ dans $\mathbf{k}^n$ permet de munir $V(\mathbf{k})$ de la topologie induite par la topologie produit sur $V(\mathbf{k})$. Pour cette topologie, les morphismes $\Phi : V \to W$ dans $\mathbf{Aff}_{\mathbf{k}}$ induisent des applications continues. Il suffit en effet de vérifier que toute application polynomiale sur $\mathbf{k}^n$, plutôt que $V(\mathbf{k})$, est continue, ce qui résulte de la continuité des opérations du corps $\mathbf{k}$. C'est une topologie localement compacte.

En particulier la topologie sur $V(\mathbf{k})$ est compatible aux changement de systèmes de coordonnées. Nous mentionnerons cette topologie par le qualificatif *ultramétrique*, car elle donnée par la métrique induite par la métrique produit sur $\mathbf{k}^n$, qui est une métrique ultramétrique sur $V(k)$. Lorsque G est un groupe affine sur $\mathbf{k}$, la topologie ultramétrique sur $G(\mathbf{k})$ est une topologie de groupe.

Appendice D
Espace analytique

D.1. Semi-normes multiplicatives homogènes. — Soit $\mathbf{k}$ un corps local muni d'une valeur absolue ultramétrique $|-|$. Sur une $\mathbf{k}$-algèbre commutative unifère A, on appelle semi-norme multiplicative une application *non constante* $\|-\| : A \to \mathbf{R}$ qui soit multiplicative, c.-à-d. telle que

$$\forall f, g \in A, \|fg\| = \|f\| \cdot \|g\| \tag{24}$$

et vérifiant l'inégalité triangulaire

$$\forall f, g \in A, \|f+g\| \leq \|f\| + \|g\|. \tag{25}$$

Une telle application transporte l'unité 1_A sur 1 et l'élément nul 0_A sur 0. Elle est dite $(\mathbf{k}, |-|)$*-homogène*, ou simplement *homogène* lorsque

$$\forall \lambda \in \mathbf{k}, \forall f \in A, \|\lambda \cdot g\| \leq |\lambda| \cdot \|f\|. \tag{26}$$

Par multiplicativité, il revient au même d'imposer que $\|-\|$ étende $|-|$, au sens où $\|\lambda \cdot 1_A\| = |\lambda|$.

D.2. Analytification. — Soit V une variété algébrique affine sur $\mathbf{k}$. Suivant V. Berkovich, [**Ber90**] 1.5.1, nous appellerons espace analytique associé à V l'espace topologique V^{an} formé de l'ensemble des semi-normes multiplicatives homogènes sur $\mathbf{k}[V]$, pour la topologie de la convergence simple. Ce sont aussi les espaces topologiques sous-jacents à certains espaces analytiques que V. Berkovich définit en [**Ber90**] 3.1 (cf. [**Ber90**] 3.4.2). Pour toute fonction régulière f sur V, nous notons $|f|$ la fonction réelle $x \mapsto x(f)$ sur V^{an}. Par définition, la topologie sur V^{an} est la plus grossière pour laquelle, pour toute fonction régulière f, la fonction $|f| : V^{\mathrm{an}} \to \mathbf{R}$ est continue.

La construction de l'espace analytique associé est fonctorielle, et covariante, de la catégorie $\mathbf{Aff}_{\mathbf{k}}$ dans celle des espaces topologiques. En effet tout morphisme $A \to A'$ dans $\mathbf{Alg}_{\mathbf{k}}$ permet, par composition, de produire une semi-norme multiplicative $A \to \mathbf{R}$ à partir d'une semi-norme multiplicative homogène sur $A' \to \mathbf{R}$. Cette opération est bien sûr compatible à la convergence simple. Pour tout morphisme Φ entre variétés algébriques affines, nous notons Φ^{an} l'application continue correspondante $V^{\mathrm{an}} \to V'^{\mathrm{an}}$.

Soit $\mathbf{k}'$ une extension finie de $\mathbf{k}$, et étendons la valeur absolue de $\mathbf{k}$ à $\mathbf{k}'$. Alors pour tout point x de V à valeur dans $\mathbf{k}'$, on obtient une semi-norme multiplicative homogène en associant à toute fonction régulière f sur V le réel $|f(x)|$. On obtient ainsi une application de $V(\mathbf{k}_s)$ dans V^{an}. Cette application commute à l'action de $\mathrm{Aut}(\mathbf{k}_s/\mathbf{k})$ sur $V(\mathbf{k}_s)$. En outre pour toute extension finie $\mathbf{k}'$ de $\mathbf{k}$, cette application est continue sur $V(\mathbf{k}')$, pour la topologie ultramétrique sur $V(\mathbf{k}')$. En effet une application régulière définit une application continue sur $V(\mathbf{k})$.

La démonstration de la Proposition 2.1.15 de [**Ber90**] permet de montrer que l'image de $V(\mathbf{k}_s)$ dans V^{an} est dense.

D.3. Des tores déployés analytiques . . . — Soit T un tore déployé sur $\mathbf{k}$. On identifie l'algèbre $\mathbf{k}[T]$ des fonctions régulières sur T à l'algèbre de groupe $\mathbf{k}[X(T)]$. Tout caractère $\chi : T \to GL(1)$, définit, par composition une application additive

$$Y(T) = \mathrm{Hom}(GL(1), T) \to \mathrm{Hom}(GL(1), GL(1)) = \mathbf{Z}.$$

Par linéarité, chaque caractère définit une forme linéaire sur l'espace vectoriel réel $\Lambda = Y(T) \otimes \mathbf{R}$, que l'on notera $\lambda \mapsto \langle \chi, \lambda \rangle$. Pour tout λ dans Λ, l'application qui envoie une fonction régulière $f = \sum_{\chi \in X(T)} a_\chi \cdot \chi$ dans $\mathbf{k}[T]$ sur

$$\max_{\chi \in X(T)} |a_\chi| \cdot |\varpi|^{\langle \chi, \lambda \rangle}, \tag{27}$$

(où $|\varpi|$ est la valeur absolue d'une uniformisante ϖ de $\mathbf{k}$) définit clairement une norme homogène sur $\mathbf{k}[T]$; cette norme est multiplicative d'après [**Ber90**] 2.1

(p. 21). La formule (27) induit donc une application, que nous noterons $\lambda \mapsto \theta_T(\lambda)$, de Λ dans T^{an}.

Lorsque l'on fixe $f = \sum_{\chi \in \mathbf{Z}^N} a_\chi \cdot \chi$ dans $\mathbf{k}[T]$, et que l'on fait varier le paramètre λ, le logarithme

$$\log(|f|(\theta_T(\lambda))) = \max_{\chi \in X(T)} \left(\log|a_\chi| + \log|\varpi| \cdot \langle \chi, \lambda \rangle\right)$$

est le maximum d'un nombre fini de fonctions affines en λ. C'est donc une fonction convexe sur Λ, et c'est en particulier une fonction continue. Comme, pour toute fonction régulière f sur T, la composition de $|f|$ avec θ_T, qui est logarithmiquement convexe, est continue, l'application θ_T est continue, par définition de la topologie sur T^{an}.

D.3.1. Le groupe $T(\mathbf{k})$ agit sur T par translation. Par transport de structure il agit sur $\mathbf{k}[T]$ puis sur T^{an}. Concrètement, un élément μ de $T(\mathbf{k})$ agit sur $\mathbf{k}[T]$ en envoyant la fonction régulière

$$x \mapsto \sum_{\chi \in X(T)} a_\chi \cdot \chi(x)$$

sur la fonction régulière

$$x \mapsto \sum_{\chi \in X(T)} a_\chi \cdot \chi(x\mu^{-1}) = \sum_{\chi \in X(T)} (a_\chi \chi(\mu^{-1})) \cdot \chi(x).$$

Soit $\lambda(\mu)$ l'élément de Λ tel que l'on ait

$$\langle \chi, \lambda(\mu) \rangle = \log_{|\varpi|}(\chi(\mu))$$

pour tout χ de $X(T)$. Alors l'action de μ envoie la norme $\theta_T(\lambda)$ sur $\theta_T(\lambda - \lambda(\mu))$.

Cette action de $T(\mathbf{k})$ sur Λ par translation s'identifie à l'action considérée dans [**Tit79**], 1.2 (1), où $\log_{|\varpi|}(\chi(\mu))$ est noté $\omega(\chi(z))$.

D.4. ...aux groupes algébriques affines. — Soit $\Phi : T \to G$ un morphisme de variétés algébriques affines du tore T dans un groupe algébrique affine G. Composant $\theta_T : \Lambda \to T^{\mathrm{an}}$ par $\Phi^{\mathrm{an}} : T^{\mathrm{an}} \to G^{\mathrm{an}}$, nous obtenons une application continue de Λ dans G^{an}. En outre, pour toute fonction régulière f sur G, la fonction réelle $|f| \circ \Phi^{\mathrm{an}} \circ \theta_T$ sur Λ s'identifie avec $|f \circ \Phi| \circ \theta_T$, et est par conséquent logarithmiquement convexe.

Notons que l'action à droite du groupe $G(\mathbf{k})$ sur la variété G induit par une fonctorialité une action de $G(\mathbf{k})$ sur G^{an}. En particulier nous pouvons définir l'application $(\Phi^{\mathrm{an}} \circ \theta_T) \cdot g$ translatée de $\Phi^{\mathrm{an}} \circ \theta_T$ par g pour tout g dans $G(\mathbf{k})$.

D.4.1. Nous allons généraliser cette construction aux éléments de $G(\mathbf{k}_s)$.

Pour toute extension séparable finie $\mathbf{k}'$ de $\mathbf{k}$, T définit un tore déployé $T_{\mathbf{k}'} = T \otimes_{\mathbf{k}} \mathbf{k}'$ sur $\mathbf{k}'$, d'algèbre $\mathbf{k}'[T_{\mathbf{k}'}] = \mathbf{k}[T] \otimes_{\mathbf{k}} \mathbf{k}'$ isomorphe à $\mathbf{k}'[X(T)]$. Par restriction des normes de $\mathbf{k}'[T_{\mathbf{k}'}]$ à $\mathbf{k}[T]$ on construit une application $T^{\mathrm{an}}_{\mathbf{k}'} \to T$. La formule (27) s'étend à $\mathbf{k}'[T_{\mathbf{k}'}]$ et définit encore norme *multiplicative* ([**Ber90**], 2.1 (p. 21)) homogène. Nous obtenons ainsi une application $\Theta_{T_{\mathbf{k}'}} : \Lambda \to T^{\mathrm{an}}_{\mathbf{k}'}$, dont la composée

avec l'application $T^{\mathrm{an}}_{\mathbf{k}'} \to T^{\mathrm{an}}$, redonne l'application θ_T. De surcroît cette extension est compatible aux morphismes d'extension $\mathbf{k} \to \mathbf{k}' \to \mathbf{k}''$.

Nous en tirons une conséquence. Si g est un élément dans $G(\mathbf{k}')$, faisons agir g à droite sur le foncteur des points de G sur $\mathbf{Alg}_{\mathbf{k}'}$: pour A dans $\mathbf{Alg}_{\mathbf{k}'}$, g agit par translation à droite sur le groupe $G(A)$, *via* son image par $G(\mathbf{k}') \to G(A)$. Il correspond une action, disons α_g, de g sur l'algèbre $\mathbf{k}'[G]$. D'où, par composition, un morphisme $\mathbf{k}[G] \to \mathbf{k}'[G] \xrightarrow{\alpha_g} \mathbf{k}'[G] \xrightarrow{\Phi_{\mathbf{k}'}} \mathbf{k}'[T]$. Ainsi, pour chaque λ dans Λ, de la norme multiplicative homogène correspondante sur $\mathbf{k}'[T] \to \mathbf{R}$ (cf. *supra*), on déduit, par composition, une norme multiplicative homogène sur $\mathbf{k}[G]$. Nous noterons $(\Phi^{\mathrm{an}} \circ \theta_T)g$ l'application de Λ dans G^{an} ainsi obtenue.

Cette construction est manifestement compatible aux extensions : si $\mathbf{k}''$ est une extension finie de $\mathbf{k}'$ et g'' l'image de g dans $G(\mathbf{k}'')$, alors $(\Phi^{\mathrm{an}} \circ \theta_T) \cdot g = (\Phi^{\mathrm{an}} \circ \theta_T) \cdot g''$. Elle ne dépend donc que de l'image de g dans $G(\mathbf{k}_s)$, peut importe le morphisme $\mathbf{k}' \to \mathbf{k}_s$. Autrment dit cette construction ne dépend que de l'image de $G(\mathbf{k}_s)$ dans G^{an}.

Pour f dans $\mathbf{k}'[T]$, la formule (27) définit encore une fonction convexe de λ. Il en résulte que pour f dans $\mathbf{k}[G]$ et g dans $G(\mathbf{k}')$, la composée $|f| \circ ((\Phi^{\mathrm{an}} \circ \theta_T) \cdot g)$ est une fonction convexe sur Λ. Ainsi l'application $(\Phi^{\mathrm{an}} \circ \theta_T) \cdot g$ est continue.

D.4.2. Étendons maintenant cette construction aux éléments p de G^{an}.

Soit un point p de G^{an} ; ce point est dans l'adhérence de l'image de $G(\mathbf{k}_s)$ dans G^{an}. Nous construire alors l'application $(\Phi^{\mathrm{an}} \circ \theta_T) \cdot p$ comme limite simple de fonctions de la forme $(\Phi^{\mathrm{an}} \circ \theta_T) \cdot g$, avec g dans $G(\mathbf{k}_s)$, lorsque l'image de g dans G^{an} tend vers p.

Montrons que cette limite simple existe et est unique.

Démonstration. — Notons $G_{\mathbf{k}_s}$ le groupe algébrique affine sur $\mathbf{k}_s$ d'algèbre $\mathbf{k}[G] \otimes_{\mathbf{k}} \mathbf{k}_s$, $T_{\mathbf{k}_s}$ le tore déployé sur $\mathbf{k}_s$ d'algèbre $\mathbf{k}[T] \otimes_{\mathbf{k}} \mathbf{k}_s$, et $\Phi_{\mathbf{k}_s}$ le morphisme $T_{\mathbf{k}_s} \to G_{\mathbf{k}_s}$ issu de Φ. Soit λ dans Λ, soit f dans $\mathbf{k}[G]$, et notons, pour tout g dans $G(\mathbf{k}_s)$, $f \circ (\Phi_{\mathbf{k}_s} \cdot g) = \sum_{\chi \in X(T)} a_\chi(g)\chi$ la fonction de $\mathbf{k}_s[X(T)]$ qui s'obtient en translatant $\Phi_{\mathbf{k}_s} : T_{\mathbf{k}_s} \to G_{\mathbf{k}_s}$ par g puis en composant par f. Tout revient à montrer que lorsque l'image de g converge dans G^{an}, le nombre réel

$$\max_{\chi \in X(T)} |a_\chi(g)| \cdot |\varpi|^{\langle \chi, \lambda \rangle}$$

tend vers une valeur limite.

Par définition, $|h(g)|$ tend vers une valeur limite pour toute fonction régulière h sur G définie sur $\mathbf{k}$. Il suffit donc de montrer que sauf pour un nombre fini de caractères χ, les fonctions $g \mapsto a_\chi(g)$ sont nulles et que, pour tout caractère χ de T, $g \mapsto a_\chi(g)$ définit une fonction régulière. Cela résulte de ce que l'action de $G(\mathbf{k}_s)$ sur $\mathbf{k}_s[G]$ est union de sous-espaces stables $\mathrm{Aut}(\mathbf{k}_s/\mathbf{k})$-invariants de dimension finie, et que l'action de $G(\mathbf{k}_s)$ sur un sous-espace stable provient d'une représentation de G définie sur $\mathbf{k}$ ([**Bor91**], 1. §1. 1.9). □

Comme une limite simple de fonctions convexes est convexe, pour tout f dans $\mathbf{k}[G]$, la composée $|f| \circ ((\Phi^{\mathrm{an}} \circ \theta_T) \cdot g)$ est une fonction convexe sur Λ. En particulier c'est une fonction continue. Par conséquent $(\Phi^{\mathrm{an}} \circ \theta_T) \cdot p$ est continue.

D.5. Un Critère. — Pour toute extension finie $\mathbf{k}'$ de $\mathbf{k}$, notons $G_{\mathbf{k}'}$ la variété algébrique affine sur $\mathbf{k}'$ associée à l'algèbre de type fini $\mathbf{k}[G] \otimes_{\mathbf{k}} \mathbf{k}'$ et $G^{\mathrm{an}}_{\mathbf{k}'}$ l'espace analytique correspondant. Notons que $G(\mathbf{k}')$ est naturellement un groupe algébrique affine sur $\mathbf{k}'$: son foncteur de point s'écrit $G_{\mathbf{k}'}(A) = G(A)$ pour A dans $\mathbf{Alg}_{\mathbf{k}'}$.

L'application $\mathbf{k}[G] \to \mathbf{k}[G] \otimes_{\mathbf{k}} \mathbf{k}'$ induit par restriction des semi-normes, une application continue $G^{\mathrm{an}}_{\mathbf{k}'} \to G^{\mathrm{an}}$. Ces applications sont manifestement compatibles aux extensions.

Notons que le morphisme $\Phi : T \to G$ induit un morphisme $\Phi_{\mathbf{k}'} : T_{\mathbf{k}'} \to G_{\mathbf{k}'}$, d'où une application continue $\Phi^{\mathrm{an}}_{\mathbf{k}'} : T^{\mathrm{an}}_{\mathbf{k}'} \to G^{\mathrm{an}}_{\mathbf{k}'}$. Le relèvement $\Lambda \to T^{\mathrm{an}}_{\mathbf{k}'}$ de $\theta_T : \Lambda \to T^{\mathrm{an}}$ obtenu en étendant la formule (27) est lui aussi compatibles aux extensions.

Proposition D.1. *— Soit $\theta : \Lambda \to G^{\mathrm{an}}$ une application continue. Supposons que pour toute extension finie $\mathbf{k}'$, il existe $\theta_{\mathbf{k}'} : \Lambda \to G^{\mathrm{an}}_{\mathbf{k}'}$ telle que*

a. *θ soit la composée de $\theta_{\mathbf{k}'}$ avec l'application $G^{\mathrm{an}}_{\mathbf{k}'} \to G^{\mathrm{an}}$ ci-dessus.*
b. *Pour tout μ dans $T(\mathbf{k}')$, l'action par translation à gauche de t sur la fonction $\theta_{\mathbf{k}'}$ commute à l'action de $T(\mathbf{k}')$ sur Λ :*

$$\theta_{\mathbf{k}'}(x) \cdot \Phi(t) = \theta(\mathbf{k}' - \lambda(\mu)). \tag{28}$$

Alors θ est l'application $(\Phi^{\mathrm{an}} \circ \theta_T) \cdot p$ où p est le point $\theta(0)$.

Démonstration. — Par limite simple on peut supposer que p est dans l'image de $G(\mathbf{k}_s)$, puis quitte à considérer une extension finie, que p appartient à $G(\mathbf{k})$, quitte à faire agir p à droite, que p est l'élément neutre.

Par continuité de θ et θ_T il suffit de montrer $\theta(\lambda) = (\Phi^{\mathrm{an}} \circ \theta_T(\lambda))$ pour un ensemble dense de λ dans Λ.

Or l'orbite dans Λ de 0 sous l'action de $T(\mathbf{k}_s)$ est dense. Cela provient de la description de cette action pour tout corps local contenu dans $\mathbf{k}_s$ grâce à la section D.3.1 et au fait que quitte à considérer des racines de l'uniformisante d'ordre premier à la caractéristique, on peut approcher tout nombre réel positif par la valeur absolue d'éléments de $\mathbf{k}_s$.

Enfin θ et $(\Phi^{\mathrm{an}} \circ \theta_T(\lambda))$ concordent en 0 et vérifient la loi de transformation (cf. section D.3.1). □

Des sections D.3.1 et D.4 on déduit que la proposition a pour corollaire le suivant.

Corollaire D.2. *— Soit $\theta : \Lambda \to G^{\mathrm{an}}$ une application telle que dans la proposition D.1. Alors pour toute fonction régulière f sur G, la fonction réelle $|f| \circ \theta$ est logarithmiquement convexe.*

Appendice E

Immeuble euclidiens de Bruhat-Tits

E.1. Avant-propos. — L'*immeuble euclidien* de Bruhat-Tits d'un groupe algébrique semisimple G sur un corps local ultramétrique $\mathbf{k}$ est un analogue, dans le contexte ultramétrique, de l'espace riemannien symétrique L des sous-groupes compacts maximaux associé à un groupe de Lie semi-simple réel L, qui s'écrit L/K, pour un sous-groupe compact maximal K de L. Dans le contexte ultramétrique, l'analogue naïf du théorème de Cartan ne vaut plus : $G(\mathbf{k}')$ ne contient en général pas, à conjugaison près, d'unique sous-groupe compact maximal. Toutefois, du moins pour les groupe déployés, les énoncés 5.3.1 et 5.3.3 de [**Ber90**] restituent *a posteriori* cette facette de l'analogie entre immeubles et espaces symétriques.

E.2. Propriétés. — Soit $\mathbf{k}$ un corps local muni d'une valeur absolue ultramétrique $|-|$, et soit G un groupe algébrique semi-simple sur $\mathbf{k}$. L'*immeuble euclidien de Bruhat-tits* de G sur $\mathbf{k}$, ou plus simplement immeuble, désigne un certain espace métrique $\mathscr{I}(G)$ muni d'une action fidèle proprement continue du groupe topologique $G(\mathbf{k})$ (à gauche par isométries). L'immeuble est uniquement défini à unique isométrie équivariante près (cf. [**Tit79**], 2.1). Le stabilisateur de l'immeuble est réduit au centre de G. Les stabilisateurs des points de $\mathscr{I}(G)$ sont des sous-groupes dits *parahoriques* de $G(\mathbf{k})$; ils sont compacts et ouverts dans $G(\mathbf{k})$: suivant [**BT84**] (voir aussi [**Tit79**], 3.4.1), Introduction, ce sont des groupes de la forme $G(\mathscr{O}_{\mathbf{k}})$ pour certaines formes entières de G sur $\mathscr{O}_{\mathbf{k}}$ (« schémas en groupes plats prolongeant G »).

L'immeuble $\mathscr{I}(G)$ admet une famille distinguée de parties, appelées *appartements*, réunissant les propriétés suivantes.

a. L'ensemble des appartements est stable sous l'action de $G(\mathbf{k})$, et l'action de $G(\mathbf{k})$ sur l'ensemble des appartements est transitive.
b. Les appartements sont isométriques à un espace vectoriel euclidien. En particulier, pour tout appartement A, et tout g dans $G(\mathbf{k})$, l'isométrie $A \to gA$ est une application affine.
c. L'immeuble $\mathscr{I}(G)$ est réunion de ses appartements, et tout point a un voisinage formé d'une réunion finie d'appartements.
d. Le stabilisateur dans $G(\mathbf{k})$ d'un appartement donné agit via un réseau du groupe d'isométries de cet appartement.
e. Deux points quelconques de $\mathscr{I}(G)$ sont contenus dans un appartement commun ([**BT72**] 7.14.18).
f. L'immeuble $\mathscr{I}(G)$ un espace de Hadamard : l'inégalité CAT(0) est satisfaite ([**BT72**], 3.2).
g. L'immeuble $\mathscr{I}(G)$ admet une structure polysimpliciale $G(\mathbf{k})$ invariante, dont un simplexe est domaine fondamental et intersection d'appartements. Le

stabilisateur d'un appartement donné préserve un pavage issu d'une structure polysimpliciale qui s'étend en une structure polysimpliciale invariante sur $\mathscr{I}(G)$.

E.3. Avertissement. — Nous nous reposons sur [**RTW09**] pour la construction de l'immeuble de Bruhat-Tits. Les hypothèses de travail de ces auteurs sont énoncées en [**RTW09**] 1.3.4, numéro qui, par ailleurs, indique explicitement que ces hypothèse sont vérifiées si le corps de base $\mathbf{k}$ est un corps local, ce qui est le cas considéré ici. Une autre référence dans le cas des corps locaux est [**Tit79**]. Cette dernière, reposant sur l'exposé axiomatique [**BT72**], indique, en [**Tit79**] 1.5, quelques réserves sur la satisfiabilité des hypothèses de [**BT72**], qui sont ramenées, en ce qui concerne [**Tit79**], aux propriétés 1.4.1 et 1.4.2 de [**Tit79**]. La suite [**BT84**] de l'exposé [**BT72**], suite postérieure à la référence [**Tit79**], démontre que les hypothèses de [**BT72**] sont satisfaites « pour tout groupe réductif sur un corps de valuation discrète hensélien à corps résiduel parfait » (Introduction, page 9).

Nous esquissons la construction de l'immeuble indiquée dans [**RTW09**]. Que cette construction vérifie les propriétés indiquée plus haut résulte, pour certaines de ces propriétés de la construction même, qui procède par analyse-synthèse. Pour les autres propriétés cela résulte d'une part de la satisfiabilité des hypothèse de travail de [**BT72**] pour les corps locaux pour laquelle nous venons d'indiquer des références ; d'autre part de certaines conclusions de [**BT72**] ; enfin, dans le cas des corps locaux notamment, de la référence [**Tit79**].

E.4. Construction. — Comme tout appartement A de l'immeuble $\mathscr{I}(G)$ est une partie génératrice, on peut construire $\mathscr{I}(G)$ comme quotient de $G(\mathbf{k}) \times A$. Les relations par lesquelles on quotiente sont engendrées par celles qui définissent le stabilisateur de chaque point de A, et celles qui déterminent l'action sur A du stabilisateur de A. C'est l'approche utilisée dans [**RTW09**] 1.3.

Ne discutons que du modèle de A muni de l'action de son stabilisateur. Fixons un tore déployé maximal T de G, et posons $A = \Lambda = \mathrm{Hom}(GL(1), T) \otimes \mathbf{R}$. Le normalisateur $N(T)(\mathbf{k})$ de T dans $G(\mathbf{k})$ agit par transport de structure sur $\Lambda = \mathrm{Hom}(GL(1), T) \otimes \mathbf{R}$, et le noyau de cette action est le centralisateur $C(T)(\mathbf{k})$ de T dans $G(\mathbf{k})$. Le quotient $N(T)(\mathbf{k})/C(T)(\mathbf{k})$ est un groupe fini, le *groupe de Weyl sphérique* de G relatif à T. Alors le stabilisateur de l'appartement A dans $G(\mathbf{k})$ est $N(T)(\mathbf{k})$ et l'action de $N(T)(\mathbf{k})$ est une action affine dont la partie linéaire est l'action précédente, pour laquelle $T(\mathbf{k})$, qui est contenu dans $N(T)(\mathbf{k})$, agit par (D.5).

Appendice F
Convexité

F.1. Notion de convexité. — Rappelons qu'un *appartement* de $\mathscr{I}_{\mathbf{k}}(G)$ l'image d'une partie de la forme $\{g\} \times \Lambda$ par l'application quotient $G(\mathbf{k}) \times \Lambda \to \mathscr{I}_k(G)$. Les appartements sont permutés transitivement sous l'action de $G(\mathbf{k})$. En outre le stabilisateur d'un appartement A agit sur A de manière affine et cette action contient l'action additive de d'un réseau vectoriel de Λ ([**Tit79**], 1.2, 1.3).

F1.1. En particulier, si F est un parallélotope fondamental de ce réseau, F est une partie bornée qui rencontre toute orbite de $G(\mathbf{k})$ rencontrant cet appartement, c'est-à-dire toute orbite de $G(\mathbf{k})$. L'immeuble $\mathscr{I}(G)$ contient donc une partie génératrice compacte.

Rappelons que deux points quelconques x et y de $\mathscr{I}_{\mathbf{k}}(G)$ sont contenus dans un appartement commun ([**BT72**] 7.14.18). On peut donc définir le segment $[x; y]$ joignant x à y dans A. Comme le stabilisateur d'un appartement A agit de manière affine sur A, ni le segment $[x, y]$, ni la structure affine sur $[x, y]$ ne dépend de l'appartement choisi (cf.[**Tit79**] 2.2.1).

Une fonction réelle continue sur $\mathscr{I}_{\mathbf{k}}(G)$ dont la restriction à tout segment est convexe (resp. affine), sera dite *convexe* (resp. *affine*). Il revient au même de dire que la restriction à chaque appartement est convexe (resp. affine), relativement à la structure affine de cet appartement.

Bien évidemment, les fonctions affines et les fonctions dont le logarithme est affine sont convexes. En outre, toute fonction réelle qui s'écrit comme borne supérieure ou limite simple de fonctions convexes est convexe.

Une partie de $\mathscr{I}(G)$ sera dite *convexe* si elle contient tout segment dont elle contient les extrémités.

F.2. Une Décomposition de l'immeuble. — Soit k un sous-groupe compact de $G(\mathbf{k})$. Le groupe compact k agit par isométries sur l'immeuble $\mathscr{I}(G)$. Notons $\mathscr{I}(G)^k$ le lieu fixe de l'action de k, et $Z(k)$ le centralisateur de k dans G. Alors $\mathscr{I}(G)^k$ est stable sous l'action du centralisateur $Z(k)(\mathbf{k})$ de k dans $G(\mathbf{k})$. Nous allons montrer le premier énoncé suivant.

Théorème F.1*. — Soit k un sous-groupe compact de $G(\mathbf{k})$ dont l'adhérence de Zariski dans G est un sous-groupe réductif, et soit $Z_G(k)$ le centralisateur de k dans G. Alors il existe une partie compacte non vide C de $\mathscr{I}(G)^k$ qui est génératrice pour l'action de $Z_G(k)(\mathbf{k})$.*

Commençons par un lemme.

Lemme F.2*. — Soit k un sous-groupe compact de $G(\mathbf{k})$ dont l'adhérence de Zariski dans G est un sous-groupe réductif, et soit $Z(k)$ le centralisateur de k dans G.*

Pour tout compact C de $G(\mathbf{k})$, il existe un compact C' de $G(\mathbf{k})$ tel que le transporteur

$$T(k,C) = \{g \in G(\mathbf{k}) \mid gkg^{-1} \subseteq C\}$$

de k dans C s'écrive $C' Z_G(k)(\mathbf{k})$.

Démonstration. — Tout d'abord ce transporteur est fermé. C'est l'intersection des fermés suivants. Pour chaque x dans k l'application $g \mapsto gxg^{-1}$ étant continue, l'image inverse de C est fermée. Tout revient donc à montrer que $T(k,C)$ est le saturé par $Z_G(k)(\mathbf{k})$ d'une partie relativement compacte. Comme $T(k,C)$ est manifestement invariant par $Z_G(k)(\mathbf{k})$, il suffit de montrer qu'il est contenu dans le saturé d'une partie compacte.

Remarquons que, pour la topologie de Zariski, k est noethérien. Par conséquent, pour cette topologie, il est topologiquement de type fini. En particulier, il existe une partie finie $\{x_1;\ldots;x_n\}$ topologiquement génératrice de k pour la topologie de Zariski. Le centralisateur de cette partie est le centralisateur de k, c'est-à-dire $Z_G(k)$.

Appliquant [**PR94**], Théorème 2.16, on montre que l'application

$$g \mapsto (gx_1g^{-1};\ldots;gx_ng^{-1})$$

induit une immersion fermée de $G/Z_G(k)$ dans G^n. Par conséquent, l'application correspondante

$$\phi : (G/Z_G(k))(\mathbf{k}) \to G(\mathbf{k})^n$$

est *propre*. En particulier l'image inverse de C^n dans $(G/Z_G(k))(\mathbf{k})$ est compacte. Or cette image inverse contient l'image de $T(k,C)$ par $G(\mathbf{k}) \to (G/Z_G(k))(\mathbf{k})$.

Il suffit donc de montrer que tout compact de $(G/Z_G(k))(\mathbf{k})$ rencontre l'image de ϕ en l'image d'un compact. D'après [**PR94**], l'application ϕ est ouverte, et les orbites de $G(\mathbf{k})$ dans $(G/Z_G(k))(\mathbf{k})$ sont toutes ouvertes ; elles sont donc aussi toutes fermées. En particulier l'image de ϕ est fermée, et intersecte donc tout compact en un compact. Il suffit donc de montrer que tout compact de $G(\mathbf{k})/Z(\mathbf{k})$ est l'image d'un compact. D'après la propriété de Borel Lebesgue, il suffit de travailler localement. Or ϕ est ouverte et $G(\mathbf{k})$ est localement compact.

□

Avant de démontrer le Théorème F.1, rappelons quelques faits, dont certains sont bien connus.

a. Il existe un compact F de $\mathscr{I}(G)$ rencontrant toute orbite de $G(\mathbf{k})$ (cf. F.1.1).
b. Pour toute partie bornée non vide P de $\mathscr{I}(G)$, le stabilisateur de P dans $G(\mathbf{k})$ est un sous-groupe compact et ouvert (cf.[**Tit79**] 3.2, [**BT72**] Introduction). En particulier, pour tout point p de $\mathscr{I}_{\mathbf{k}}(G)$, le fixateur de p dans $G(\mathbf{k})$ est un sous-groupe compact et ouvert.
c. Le fixateur commun à tous les éléments d'une partie bornée non vide est compact et ouvert (cf. *supra*).

d. Pour tout sous-groupe ouvert U de $G(\mathbf{k})$, le lieu fixe de U dans G est une partie compacte de $\mathscr{I}(G)$.
e. Tout sous-groupe compact de $G(\mathbf{k})$ est contenu dans un sous-groupe compact maximal.
f. Les sous-groupes compacts maximaux de $G(\mathbf{k})$ sont ouverts.
g. Ils forment un nombre fini de classes de conjugaison ([**BT72**] 3.3.3).
h. Tout sous-groupe compact ouvert de $G(\mathbf{k})$ est contenu dans un nombre fini de sous-groupe compact maximaux.

Démonstration du théorème F.1. — D'après le point *a.*, il existe un compact F de $\mathscr{I}(G)$ rencontrant toute orbite de $G(\mathbf{k})$. D'après le point *b.*, le stabilisateur commun à tous les points de F est un sous-groupe *compact et ouvert* de $G(\mathbf{k})$. Notons-le K_F.

Pour tout point f de F le stabilisateur de f, disons K_f, est également un sous-groupe *compact et ouvert* de $G(\mathbf{k})$ (point *b.* ci-dessus). Par construction ces groupes contiennent K_F. Appliquant le point *h.*, il s'ensuit que l'ensemble $E_F = \{K_f | f \in F\}$ de sous-groupes compacts et ouverts de $G(\mathbf{k})$ est un ensemble *fini*.

Pour K dans E_F, notons $F_K = \{f \in F | K_f = K\}$. Par construction de E_F, le compact F s'écrit comme l'union finie $F = \bigcup\{F_K | K \in E_F\}$. Notons que chaque F_K, étant contenu dans F, est borné.

Soit k le groupe compact mentionné dans l'énoncé du théorème. Pour g dans $G(\mathbf{k})$ et f dans F_K, le point gf de $\mathscr{I}(G)$ est fixé par k si et seulement si $g^{-1}kg$ est contenu dans le stabilisateur de f, c'est-à-dire dans K. Autrement dit g^{-1} est dans le transporteur $T(k,K)$ de k dans K.

D'après le Lemme F.2, il existe un compact C_K de $G(\mathbf{k})$ tel que $T(k,K)$ s'écrive $C_K Z_G(k)$. Par conséquent, l'élément gf ci-dessus appartient à la partie $Z_G(k)(\mathbf{k}) \cdot {C_K}^{-1} \cdot F_K$ de $\mathscr{I}(G)^k$.

On a montré que tout point de la forme gf, avec g dans $G(\mathbf{k})$ et f dans F_K appartient en fait à $Z_G(k)(\mathbf{k}) \cdot {C_K}^{-1} \cdot F_K$.

Comme F rencontre toute orbite de $G(\mathbf{k})$ dans $\mathscr{I}(G)$, tout point p de $\mathscr{I}(G)$ s'écrit fg avec f dans F et g dans $G(\mathbf{k})$. Ainsi tout point fixe de k appartient à $Z_G(k)(\mathbf{k}) \cdot {C_K}^{-1} \cdot F_K$ pour un certain K dans E_F. Par conséquent, $\mathscr{I}(G)^k$ est contenu dans $\bigcup_{K \in E_F} Z_G(k)(\mathbf{k}) \cdot {C_K}^{-1} \cdot F_K$.

Comme E_F est fini et que les F_K et C_K sont bornés, la partie $\bigcup_{K \in E_F} Z_G(k)(\mathbf{k}) \cdot {C_K}^{-1} \cdot F_K$ est bornée, donc son adhérence est compacte. Remarquons que $\mathscr{I}(G)^k$ est fermé et invariant sous l'action de $Z_G(k)(\mathbf{k})$. Par conséquent

$$C = \overline{\bigcup_{K \in E_F} {C_K}^{-1} \cdot F_K} \cap \mathscr{I}(G)^k$$

est un compact de $\mathscr{I}(G)$ tel que $\mathscr{I}(G)^k = C Z_G(k)(\mathbf{k})$. □

F.3. Plongement analytique et Convexité des fonctions régulières l'immeuble. — Nous basant sur [**RTW09**], démontrons l'énoncé suivant.

Théorème F.3. — *Soit* $\mathbf{k}$ *un corps local muni d'une valeur absolue ultramétrique, soit* G *un groupe algébrique semi-simple sur* $\mathbf{k}$ *et fixons un tore algébrique déployé maximal* T *dans* G*. Notons* $\Phi : T \to G$ *le morphisme d'inclusion,* $\theta_T : \Lambda \to T^{\mathrm{an}}$ *l'application (27),* $\Phi^{\mathrm{an}} : T^{\mathrm{an}} \to G^{\mathrm{an}}$ *l'application correspondante, et* $\mathscr{I}(G)$ *l'immeuble de Bruhat-Tits de* G *sur* $\mathbf{k}$*. Pour tout point* p *de* G^{an}*, on note* $((\Phi^{\mathrm{an}} \circ \theta_T) \cdot p) : \Lambda \to G^{\mathrm{an}}$ *l'application définie dans la section D.4, et pour tout* g *dans* $G(\mathbf{k})$*, on note* $g((\Phi^{\mathrm{an}} \circ \theta_T) \cdot p)$ *l'application translatée.*

Alors il existe un point p *de* G^{an} *tel que l'application de* $G(\mathbf{k}) \times \Lambda$ *donnée par*

$$(g, \lambda) \mapsto g \cdot ((\Phi^{\mathrm{an}} \circ \theta_T) \cdot p)(\lambda) \tag{29}$$

passe au quotient en une application équivariante à gauche

$$\theta : \mathscr{I}(G) \to G^{\mathrm{an}}.$$

En outre on peut supposer que p *le stabilisateur à droite* G_p *de* p *dans* $G(\mathbf{k})$ *est compact et ouvert.*

Dans le cas déployé, cet énoncé résulte de la construction explicite de V. Berkovich, dans [**Ber90**], 5.3 et du théorème 5.4.2 qui suit.

Dans le cas général, notre référence est [**RTW09**], dont l'approche est différente, et repose sur les propriétés de fonctorialité des immeubles par des extensions, non nécessairement algébriques, de corps ultramétriques. Pour pouvoir démontrer l'énoncé F.3, nous allons utiliser le critère D.1.

Démonstration. — Soit $\Theta : \mathscr{I}(G) \times \mathscr{I}(G) \to G^{\mathrm{an}}$ l'application de [**RTW09**] 2.3. D'après [**RTW09**], Proposition 2.12, l'application Θ est continue et vérifie

$$\forall x, y \in \mathscr{I}(G), \forall g, h \in G(\mathbf{k}), \Theta(gx, hy) = h\Theta(x, y)g^{-1}.$$

Soit o dans $\mathscr{I}(G)$ et notons Θ_o l'application $x \mapsto \Theta(o, x)$. Alors Θ_o est une application continue et équivariante de $\mathscr{I}(G)$ dans G^{an}. Montrons que Θ_o répond à l'énoncé.

Par équivariance, il suffit donc de montrer qu'elle s'écrit sous la forme (29) sur un seul appartement, par exemple Λ, de $\mathscr{I}(g)$.

Il suffit donc de montrer que la restriction de Θ_o à Λ vérifie le critère D.1. L'application Θ_o est bien continue. Soit $\mathbf{k}'$ une extension finie de $\mathbf{k}$, et soit $\Theta_{\mathbf{k}'}$ l'application composée issue du coin supérieur gauche du carré commutatif de [**RTW09**], Proposition 2.12 (ii). Par commutativité, l'application $(\Theta_{\mathbf{k}'})_o : x \mapsto \Theta_{\mathbf{k}'}(o, x)$ de Λ dans $G^{\mathrm{an}}_{\mathbf{k}'}$ répond à la condition 1 de D.1. Appliquant la proposition 2.12 de [**RTW09**] au corps $\mathbf{k}'$, la nous obtenons que l'application $(\Theta_{\mathbf{k}'})_o$ est $T(\mathbf{k}')$-équivariante à gauche sur Λ. La seconde condition de la Proposition D.1 découle ainsi de la description de l'identité de l'action de $T(\mathbf{k}')$ sur Λ, pris comme appartement (cf. section E.4), avec l'action donnée en (cf. section D.3.1). □

En appliquant le Corollaire D.2, on en déduit.

Corollaire F.4. — *Soit* Θ *une application* $\mathscr{I}(G) \to G^{\mathrm{an}}$ *telle que dans le Théorème F.3.*

Alors pour toute fonction régulière f *sur* G*, la fonction réelle* $|f| \circ \Theta$ *est logarithmiquement convexe sur* $\mathscr{I}(G)$*.*

Références

[Ber90] V. G. BERKOVICH – *Spectral theory and analytic geometry over non-Archimedean fields*, Mathematical Surveys and Monographs, vol. 33, American Mathematical Society, Providence, RI, 1990.

[Bor91] A. BOREL – *Linear algebraic groups*, second éd., Graduate Texts in Mathematics, vol. 126, Springer-Verlag, New York, 1991.

[Bou60] N. BOURBAKI – *Éléments de mathématique. XXVI. Groupes et algèbres de Lie. Chapitre 1 : Algèbres de Lie*, Actualités Sci. Ind. No. 1285. Hermann, Paris, 1960.

[Bou63] _____, *Éléments de mathématique. Fascicule XXIX. Livre VI : Intégration. Chapitre 7 : Mesure de Haar.*, Actualités Scientifiques et Industrielles, No. 1306, Hermann, Paris, 1963.

[BT65] A. BOREL & J. TITS – « Groupes réductifs », *Inst. Hautes Études Sci. Publ. Math.* (1965), no. 27, p. 55–150.

[BT72] F. BRUHAT & J. TITS – « Groupes réductifs sur un corps local », *Inst. Hautes Études Sci. Publ. Math.* (1972), no. 41, p. 5–251.

[BT84] _____, « Groupes réductifs sur un corps local. II. Schémas en groupes. Existence d'une donnée radicielle valuée », *Inst. Hautes Études Sci. Publ. Math.* (1984), no. 60, p. 197–376.

[Dem76] M. DEMAZURE – « Démonstration de la conjecture de Mumford (d'après W. Haboush) », in *Séminaire Bourbaki (1974/1975 : Exposés Nos. 453–470), Exp. No. 462*, Springer, Berlin, 1976, p. 138–144. Lecture Notes in Math., Vol. 514.

[Gro60] A. GROTHENDIECK – « Éléments de géométrie algébrique. I. Le langage des schémas », *Inst. Hautes Études Sci. Publ. Math.* (1960), no. 4, p. 228.

[Mos55] G. D. MOSTOW – « Some new decomposition theorems for semi-simple groups », *Mem. Amer. Math. Soc.* **1955** (1955), no. 14, p. 31–54.

[PR94] V. PLATONOV & A. RAPINCHUK – *Algebraic groups and number theory*, Pure and Applied Mathematics, vol. 139, Academic Press Inc., Boston, MA, 1994, Translated from the 1991 Russian original by Rachel Rowen.

[Ric09] R. RICHARD – « On narrowness for S-arithmetic translates », *Cette thèse* (2009).

[RS09] R. RICHARD & N. SHAH – « Résultat géométrique sur les représentations de groupes de Lie réductifs », *Cette thèse* (2009).

[RTW09] B. RÉMY, A. THUILLIER & A. WERNER – « Bruhat-Tits theory from Berkovich's point of view. I - Realizations and Compactifications of buildings », *Prépublication* (2009).

[Ser68] J.-P. SERRE – *Corps locaux*, Hermann, Paris, 1968, Deuxième édition, Publications de l'Université de Nancago, No. VIII.

[Tit79] J. TITS – « Reductive groups over local fields », in *Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis,*

Ore., 1977), Part 1, Proc. Sympos. Pure Math., XXXIII, Amer. Math. Soc., Providence, R.I., 1979, p. 29–69.

[Wei74] A. WEIL – *Basic number theory*, third éd., Springer-Verlag, New York, 1974, Die Grundlehren der Mathematischen Wissenschaften, Band 144.

RODOLPHE RICHARD, IRMAR, Bâtiment 22-23, université de Rennes 1, Campus de Beaulieu, 35000 Rennes. • *E-mail :* Rodolphe.RICHARD@Normalesup.org

ON NARROWNESS FOR TRANSLATED ALGEBRAIC PROBABILITIES IN S-ARITHMETIC HOMOGENEOUS SPACES

par

Rodolphe RICHARD

In this article, we show how, along the lines of [**EMS97**], to combine

1. application of Dani-Margulis linearisation method, in the form given by D. Kleinbock and G. Tomanov in [**KT07**];
2. with the geometric results of [**RS09**] and [**Ric09**] (or rather their combination in Theorem 2.1)

in order to prove a more general and precise variant of the main result of [**EMS97**] encompassing the S-arithmetic setup (Theorem 1.1, 1.2 and 1.3 below). In particular, together with [**RS09**] and [**KT07**], this article contains a complete alternative proof of the main result of [**EMS97**]. As one of the referre observed, our result overlap the section 7 of the preprint [**BGO08**].

The result from [**KT07**] that we will use is a consequence of [**KT07**] Theorem 9.3 which is slightly more general than the an application that [**KT07**] already worked out, namely Theorem 9.4. In order to obtain this generalisation we will need to check that the lemmas from [**KT07**] allow to apply results from [**KT07**] to the case we consider. This is done in section 3 and 5. Section 4 recall some of the notations of [**KT07**] that we will use in order to express how we will use Theorems 9.3 and 9.4 of [**KT07**].

Contents

1. Non-divergence relative to semisimple S-Arithmetic lattices . . 2
2. Combination of [**RS09**] and [**Ric09**] 5
3. Preliminary Lemmas 6
4. Spaces of lattices, Mahler's criterion 8
5. A "good" parametrisation 9
6. Proof 11
References 12

1. Non-divergence relative to semisimple S-Arithmetic lattices

Let us fix once for all a *finite* set S of places of the field $\mathbf{Q}$ of rational numbers. Excluding this section, S will be assumed to contain the archimedean place. Denote the completion of $\mathbf{Q}$ at v by $\mathbf{Q}_v$ and endow the product $\mathbf{Q}_S = \prod_{v\in S}\mathbf{Q}_v$ with the "maximum" norm

$$|(a_v)_{v\in S}|_S = \max\{|a_v|\,|\,v\in S\}.$$

so the balls for the product metric below are exactly products of balls of the factors $\mathbf{Q}_v$

$$d_S((a_v)_{v\in S},(b_v)_{v\in S}) = |(a_v)_{v\in S}-(b_v)_{v\in S}|_S = \max\{|a_v-b_v|\,|\,v\in S\}.$$

We fix a natural integer m and endow the group $GL(m,\mathbf{Q}_S)$ with its natural metric topology. We consider a *smooth reductive* closed algebraic subgroup G of $GL(m)$ over $\mathbf{Q}$, and we endow $G(\mathbf{Q}_S)$ with the induced topology. Define $\mathbf{Z}_S$ to be the localised ring $\mathbf{Z}[1/p_1;\ldots;1/p_k]$, where $p_1,\ldots,p_k$ are the primes corresponding to the finite places in S. We denote by $G(\mathbf{Z}_S)$ the intersection $GL(m,\mathbf{Z}_S)\cap G(\mathbf{Q}_S)$, and for any algebraic subgroup H in G, by $H(\mathbf{Z}_S)$ the intersection $H(\mathbf{Q}_S)\cap G(\mathbf{Z}_S)$.

Recall that $G(\mathbf{Z}_S)$ is a lattice in $G(\mathbf{Q}_S)$ if and only if G has no non constant character $G\to GL(1)$ defined over $\mathbf{Q}$ (cf. [**BHC62**]). Of course, this holds for any reductive subgroup H of G instead of G. We prove the following.

Theorem 1.1. — *Assume that $G(\mathbf{Z}_S)$ is a lattice in $G(\mathbf{Q}_S)$, and consider a reductive subgroup H of G such that $H(\mathbf{Z}_S)$ is also a lattice in $H(\mathbf{Q}_S)$. Let us denote by μ_H the direct image by*

$$H(\mathbf{Z}_S)\backslash H(\mathbf{Q}_S)\to G(\mathbf{Z}_S)\backslash G(\mathbf{Q}_S) \tag{1}$$

of the $H(\mathbf{Q}_S)$-invariant probability on $H(\mathbf{Z}_S)\backslash H(\mathbf{Q}_S)$.

For any g in $G(\mathbf{Q}_S)$ we write μ_{Hg} for the direct image of the probability μ_H by the right action of g on $G(\mathbf{Z}_S)\backslash G(\mathbf{Q}_S)$.

Then the family $\left(\mu_{Hg}\right)_{g\in G}$ is narrow if and only if the centraliser of $H(\mathbf{Q}_S)$ in $G(\mathbf{Q}_S)$ has compact image in $G(\mathbf{Z}_S)\backslash G(\mathbf{Q}_S)$.

Recall that a family $(\mu_i)_{i\in I}$ of bounded positive measures on a locally compact space X is said to be narrow if for every $\epsilon>0$, there is some compact K_ϵ in X such that

$$\forall\, i\in I, \mu_i(X\smallsetminus K_\epsilon)<\epsilon. \tag{2}$$

Equivalently this family is relatively compact in the space of probabilities on X.

Theorem 1.1 will actually follows from this more general one.

Theorem 1.2. — *Let Y_S be a subset of $G(\mathbf{Q}_S)$ satisfying Theorem 2.1.*

Then the family $\left(\mu_{Hy}\right)_{y\in Y_S}$ is narrow.

Let us show how Theorem 1.1 implies Theorem 1.2.

Proof. — Let Z be the centraliser of H in G. We first show that the assumption on Z is necessary. For any compact subset C of $H(\mathbf{Q}_S)$ and any point x in the image of (1), we have $xCz = xzC$ for any z in $Z(\mathbf{Q}_S)$. Consequently, as xz go to infinity in Alexandroff compactification of $G(\mathbf{Z}_S)\backslash G(\mathbf{Q}_S)$, xCz will uniformly go to infinity. Choosing C to have positive, as we may, μ_H measure, we contradict the claimed narrowness, namely formula (2) for $\epsilon = \mu_H(C)$.

Let us now prove the sufficiency of the assumption on Z: there is a compact subset C of $Z(\mathbf{Q}_S)$ such that $Z(\mathbf{Q}_S) = Z(\mathbf{Z}_S) \cdot C$. From Theorem 2.1, the Y_S is such that $G(\mathbf{Q}_S) = Z(\mathbf{Q}_S) Y_S$. Consequently we get $G(\mathbf{Q}_S) = Z(\mathbf{Z}_S) \cdot C Y_S$.

We now remark that for any y in $Z(\mathbf{Z}_S)$, one has $\mu_{Hy} = \mu_H$. Indeed both sides are direct image of the same measure under the same map, because the composition of (1) with the action of y result in the map (1) itself: indeed, for h in $H(\mathbf{Q}_S)$,

$$G(\mathbf{Z}_S) H(\mathbf{Q}_S) y = G(\mathbf{Z}_S) y H(\mathbf{Q}_S) = G(\mathbf{Z}_S) H(\mathbf{Q}_S)$$

as y centralises H and belongs to $G(\mathbf{Z}_S)$ respectively.

Consequently the families $\left(\mu_{Hg}\right)_{g\in G}$ and $\left(\mu_{Hg}\right)_{g\in CY_S}$ have the same members. But applying Proposition 2.2 and then Theorem 1.2, we prove that the latter family $\left(\mu_{Hg}\right)_{g\in CY_S}$ is narrow, whence the desired result. □

As we may write $H(\mathbf{Q}_S) = \prod_{v\in S} H(\mathbf{Q}_v)$, and choose below for f the characteristic function of a fundamental domain (cf. [**BHC62**]) of $H(\mathbf{Z}_S)$ in $H(\mathbf{Q}_S)$ Theorem 1.2 is a particular case of the following.

Theorem 1.3. — *Assume that $G(\mathbf{Z}_S)$ is a lattice in $G(\mathbf{Q}_S)$.*

For each v in S, let $G_{\mathbf{Q}_v}$ denote the group on $\mathbf{Q}_v$ obtained by base change from $\mathbf{Q}$ to $\mathbf{Q}_v$. We consider, for each v in S, a reductive closed algebraic subgroup H_v of $G_{\mathbf{Q}_v}$, and we write $H = \prod_{v\in S} H_v(\mathbf{Q}_v)$. Let μ_H be some Haar measure on H, let f be a positive bounded (measurable) μ_H-summable real function on H and let us denote by μ_f the direct image of $f \cdot \mu_H$ by

$$H \to G(\mathbf{Z}_S)\backslash G(\mathbf{Q}_S).$$

For any g in $G(\mathbf{Q}_S)$ we write $\mu_{f\cdot g}$ for the direct image of the measure μ by the right action of g on $G(\mathbf{Z}_S)\backslash G(\mathbf{Q}_S)$.

Let Y_S be a subset of $G(\mathbf{Q}_S)$ satisfying Theorem 2.1.

Then the family $\left(\mu_y\right)_{y\in Y_S}$ is narrow.

Actually Theorem 1.3 will follow from the following *a priori* weaker corollary.

Corollary 1.4. — *There exits at least one positive essentially non zero bounded measurable μ_H-summable function f on H such that the conclusion of Theorem 1.3 holds for every subset Y_S as in Theorem 2.1.*

Let us see why Theorem 1.3 follows from Corrolary 1.4.

Proof. — We will say that a function (resp. measure) f *dominates* a function (resp. measure) g if there is a constant C such that $f \leq g$. For measures, this inequality is an inequality of functions on the Borel algebras. We will say that a family of measures $(\mu_i)_{i\in I}$ is *dominated* by an other family $(\nu_i)_{i\in I}$ on the same index set, if there is a constant C such that uniformly relative to i in I, such that $\mu_i \leq C\nu_i$.

Barycenter will means barycentre *with positive coefficients*. One readily sees on formula (2) that

(3) any family dominated by a narrow family is narrow,

(4) the family of barycentres of the elements of a narrow family is narrow,

(5) the disjunction of finitely many narrow families is a narrow family,

(6) a subfamily extracted from a narrow family is narrow,

(7) the family of limits elements of a narrow family is narrow.

Note that in the last property, we can equivalently use narrow or vague convergence. Indeed these are the same on narrow families, hence, by (6), on any converging subfamily. We will say a sequence $((\mu_{(i,n)})_{i\in I})_{n\in\mathbf{N}}$ of families of measures uniformly converges to a family $(\mu'_i)_{i\in I})$ if the mass $\left|\mu_{(i,n)}(1) - \mu'_i(1)\right|$ of $\left|\mu_{(i,n)} - \mu'_i\right|$ converges to 0, unifomrly with repect to i.One shows that

(8) If each family $((\mu_{(i,n)})_{i\in I})$ is narrow, then the familly $(\mu'_i)_{i\in I}$ is narrow.

Indeed, for each positive invertible ϵ, equation (2) is satisfied for $(\mu'_i)_{i\in I}$ if n is such that (2) it is satisfied $((\mu_{(i,n)})_{i\in I})$ with $\epsilon/2$ and $\left|\mu_{(i,n)}(1) - \mu'_i(1)\right| < \epsilon/2$ for every i in I.

Let E denote the set of positive bounded measurable μ_H-summable functions f on H such that the conclusion of Theorem 1.3 holds for every subset Y_S as in Theorem 2.1.

Applying property (3) we see that a bounded measurable μ_H-summable positive function belongs to E as soon as the characteristic function of its support belongs to E. Using properties (5) and (4) and (6), we see that E is invariant under barycentre, hence, by property (3), under positive linear combination. As every bounded measurable μ_H-summable positive function is a monotone upper limit of functions with compact support, it is enough, by (8), to prove E contain the characteristic functions of compact subsets.

We now claim that E is stable under the action of $H(\mathbf{Q}_S)$ by right translation. By Proposition 2.2, for any h in $H(\mathbf{Q}_S)$ we can replace Y_S by $\{h\}\cdot Y_S$. But Corollary 1.4 for the translated function $f\cdot h$ and the subset Y_S is equivalent to is the Corollary 1.4 for the original function $f\cdot h$ and the translated subset Y_S, whence the claim.

Consequently, using Borel-Lebesgue criterion, invariance by linear combinations and (3), E will contain every characteristic function of a compact subset as soon as it contains the characteristic function of an open subset.

Let f be a function such that in Corollary 1.4. Then there exist a point h in $H(\mathbf{Q}_s)$ such that f is essentially zero on no neighbourhood of h. Possibly translating f, we may assume that h is the neutral element. Let C' be a symmetric bounded (measurable) neighbourhood of h; then $(f\mu_H)(C') > 0$. Set $C = C' \cdot C'$, and let f_C denote the convolution of f_C with the characteristic function of C. Then one easily shows that, for any c in C', $f_C(c) \geq (f\mu_H)(C') > \epsilon$. Hence f_C dominate the characteristic function of C', and *a fortiori* the characteristic function of the nonempty interior of C'.

We will be done showing that f_C belongs to E. Let μ_C be the restriction of μ_H to C. Then f_C is proportional to the convolution of f with the probability $\frac{\mu_C}{\mu(C)}$, as $\mu(C)$ is finite and nonzero. But the latter convolution is a limit of barycentres of translates of f, hence by (4) and (7), belong to E. Consequently, by (3), f_C belongs to E, and we are done. □

Note that Theorem 1.3 is immediate if $G(\mathbf{Z}_S)\backslash G(\mathbf{Q}_S)$ is compact. From Borel and Harish-Chandra, this is the case if and only if G is anisotropic over $\mathbf{Q}$. Note also that when S does not contain the archimedean place, then $G(\mathbf{Z}_S)$ defines a lattice in $G(\mathbf{Q}_S)$ if and only if G is anisotropic over $\mathbf{R}$. In such a case G is also anisotropic over $\mathbf{Q}$.

From now on we assume that G is isotropic over $\mathbf{Q}$. Hence S contains the archimedean place. We now turn to the statement of Theorem 2.1 and the proof of Corollary 1.4.

2. Combination of [RS09] and [Ric09]

We state a direct consequence of [**RS09**] and [**Ric09**]. Compare with Theorem 1.3 for some of the notations.

Theorem 2.1. — *Consider, for each v in S, a closed reductive subgroup H_v of $G_{\mathbf{Q}_v}$ and let $H = \prod_{v\in S} H_v(\mathbf{Q}_v)$. Let Z be the centraliser of H in G. Then there exists a subset Y_S of $G(\mathbf{Q}_S)$, which is closed for the metric topology, and such that*

1. *on the one hand we have $G(\mathbf{Q}_S) = Y_S \cdot Z(\mathbf{Q}_S)$,*
2. *on the other hand, given*
   - *for each v in S, a finite dimensional $\mathbf{Q}_v$-linear representation $\rho_v : G_v \to GL(V_v)$,*
   - *for each v in S, a subset Ω_v of H such that every matrix coefficient of some of the ρ_v that cancels on Ω_v actually cancels on H_v,*
   - *for each v in S, a $\mathbf{Q}_v$-homogeneous norm $\|-\|_v$ on V_v,*

there exists a constant $c > 0$ such that,

$$\forall y \in Y, \forall (x_v)_{v\in S} \in V, \prod_{v\in S} \sup_{\omega_v\in\Omega_v} \left\|\rho(y\cdot\omega_v)(v)\right\| \geq \left(\prod_{v\in S} \|x_v\|\right) \Big/ c. \tag{9}$$

Proof. — For any v in S we get a subset Y_v of $G(\mathbf{Q}_S)$ by applying

- Theorem 1 of [**RS09**] (relative to H_v) if v is archimedean;
- Theorem 1.1 of [**Ric09**] (relative to H_v) if v is ultrametric;

and let Y be the subset of $G(\mathbf{Q}_S)$ made of the product of the Y_v.

By construction, we have $G(\mathbf{Q}_v) = Z(\mathbf{Q}_v)\cdot Y_v$ for any v in S, whence $G(\mathbf{Q}_S) = Z(\mathbf{Q}_S)\cdot Y_S$. On the other hand, for every v in S, we have, for some invertible positive constant c_v,

$$\forall y \in Y_v, \forall x_v \in V_v, \sup_{\omega\in\Omega_v} \left\|\rho_v(y_v\cdot\omega_v)(x_v)\right\|_v \geq \|x_v\|_v / c_v. \tag{10}$$

Taking the product over v in S, this yields formula (9) with $c = \prod_{v\in S} c_v$. □

Proposition 2.2. — *If Y_S is a subset of $G(\mathbf{Q}_S)$ satisfying Theorem 2.1, then, for any nonempty compact subset C of $G(\mathbf{Q}_S)$, we may replace, in Theorem 2.1, Y_S by the subset $C\cdot Y_S$.*

Proof. — We first note that Y_S being closed and C being compact, $C\cdot Y_S$ is closed in $G(\mathbf{Q}_S)$. then that $CY_SZ(\mathbf{Q}_S) = CG(\mathbf{Q}_S) = G(\mathbf{Q}_S)$, and finally that for all (a, y) in $C\times Y_S$, for all $(x_v)_{v\in S}$ in V,

$$\left(\prod_{v\in S} \|x_v\|\right) \Big/ c \leq \prod_{v\in S} \sup_{\omega_v\in\Omega_v} \left\|\rho(y\cdot\omega_v)(v)\right\| \leq \prod_{v\in S} \sup_{\omega_v\in\Omega_v} \left|\!\left|\!\left|a^{-1}\right|\!\right|\!\right|_v \left\|\rho(ay\cdot\omega_v)(v)\right\| \tag{11}$$

where $\left|\!\left|\!\left|a^{-1}\right|\!\right|\!\right|_v$ is the opertor norm of a acting on V_v. As C is compact, $\left|\!\left|\!\left|a^{-1}\right|\!\right|\!\right|_v$ is bounded on C, for any v in S, by some Λ_v. Putting $\Lambda = \prod_{v\in S}\Lambda_v$, we get

$$\left(\prod_{v\in S} \|x_v\|\right) \Big/ (c\Lambda) \leq \prod_{v\in S} \sup_{\omega_v\in\Omega_v} \left\|\rho(ay\cdot\omega_v)(v)\right\|,$$

whence theorem 2.1 for $C\cdot Y_S$ with constant $c\Lambda$ (depending on ρ_v and Ω_v). □

3. Preliminary Lemmas

We first prove some lemmas that will allow us to adapt the proof of Theorem 9.3 in [**KT07**] to our needs.

Lemma 3.1. — *Let p be a prime number, let n be a natural integer and let Φ be a finite dimensional linear subspace of $\mathbf{Q}_p(T_1,\dots,T_n)$. Assume that every ϕ is defined at the origin 0 of ${\mathbf{Q}_p}^n$. Then there exists*

- *an arbitrarily small compact neighbourhood U of 0 in $\mathbf{Q}_p^n$*
- *and a polynomial P in $\mathbf{Q}_p[T_1,\dots,T_n]$*

such that

1. $P \cdot \Phi$ *is included in* $\mathbf{Q}_p[T_1, \ldots, T_n]$
2. *and* $|P(x)| = 1$ *for any* x *in* U.

Proof. — Choose a finite basis of Φ and let P the lowest common denominator of the elements of Φ. As P is a common denominator, property 1 is satisfied. By minimality, P only cancels where some of the element of Φ is undefined. In particular $P(0)$ is nonzero, so we can renormalise P in such a way that $P(0) = 1$. Then $|P|$ is a real continuous function on $\mathbf{Q}_p^n$ which takes value 1 at 0. But A is an isolated value of $|-|$, and *a fortiori* of $|P|$. Hence $|P| = 1$ holds on a some neighbourhood of 0. Let U be such a neighbourhood, we can assume to be arbitrarily small, and in particular compact. Then P and U answer the lemma. □

Proposition 3.2. — *Let p be a prime number, let n be a natural integer and let H be a algebraic closed subgroup of $GL(n)$ over $\mathbf{Q}_p$, for some natural integer n.*

Then there exist natural integers M and d and a continuous open map $\Theta : {\mathbf{Z}_p}^d \to H(\mathbf{Q}_p)$ sending 0 to the neutral element e of H and such that for any $\mathbf{Q}_p$-linear form ϕ on $M_n(\mathbf{Q}_p)$, the real map $|\Phi \circ \Theta|$ can be written $|P|$ for some P in $\mathbf{Q}_p[T_1, \ldots, T_d]$ of degree at most M.

Proof. — Note that H is a linear algebraic group. Recall that H is a unirational variety: there exists an integer d and a dominant birational map $u : \mathbf{A}^d_{\mathbf{Q}_p} \to H$. Such a map is generically submersive, and as ${\mathbf{Q}_p}^d$ is Zariski dense in $\mathbf{A}^d_{\mathbf{Q}_p}$, there is point x in ${\mathbf{Q}_p}^d$ at which u is defined and submersive. Possibly translating by $-x$ we may assume that $x = 0$, and possibly left translating by $u(0)^{-1}$, we may assume that $u(0) = e$.

As u is submersive at 0, the corresponding map $u(\mathbf{Q}_p) : {\mathbf{Q}_p}^d \to H(\mathbf{Q}_p)$ is open on a neighbourhhod of 0. As the map $u(\mathbf{Q}_p)$ is rational, for any $\mathbf{Q}_p$-linear form ϕ on $M_d(\mathbf{Q}_p)$, the map $\phi \circ u$ is a rational function. For varying ϕ, these rational functions generate a finite dimensional linear subspace Φ of $\mathbf{Q}_p(T_1, \ldots, T_d)$ made of rational functions which are defined at 0. Applying the lemma we find a polynomial P such that $P\Phi$ is a finite dimensional linear space of polynomials. Let M be the maximum degree of these polynomials. The lemma also gives a neighbourhood U of 0, which we choose to be sufficiently so that $u(\mathbf{Q}_p)$ is open on U, such that $|P| = 1$. Then, writing $\left|\phi\right| = \left|P\phi\right| / |P|$, and using the fact that $|P| = 1$ on U, we conclude that for any $\mathbf{Q}_p$-linear form ϕ on $M_d(\mathbf{Q}_p)$, $\left|\Phi \circ u(\mathbf{Q}_p)\right|$ can be written $|P|$ for some P in $\mathbf{Q}_p[T_1, \ldots, T_d]$ of degree at most M. Then we can construct Θ such as in the proposition by composing by $u(\mathbf{Q}_p)$ any linear open immersion ${\mathbf{Z}_p}^d \to U$. If R is the positive radius of a closed ball contained in U, then $x \mapsto p^{-k}x$ whenever k is an integer that is greater than $\log_p(R)$. □

Proposition 3.3. — *Let Φ be a rational open map $\mathbf{Z}_p{}^d \to H(\mathbf{Q}_s)$. Then the direct image of the Haar measure of $\mathbf{Z}_p{}^d$ is absolutely continuous with respect to the Haar measure of $H(\mathbf{Q}_S)$.*

Proof. — One needs to show that the inverse image, say I, of a null set is a null set. As Φ is open, it is generically submersive, for the Zariski topology. As the singular locus of Φ is a strict subvariety, it is contained in the zero set of a nonzero polynomial, hence is a null set. Consequently it will be enough to show that the intersection of I with the regular locus of Φ has measure zero. It will be enough to check this locally. But locally, Φ is *analytically conjugated* to a linear map $\mathbf{Z}_p{}^d \to \mathbf{Z}_p{}^{\dim(H)}$ (we mean formally conjugated *via* locally invertible convergent power series on the considered neighbourhood.) We recall that the Haar measure on $\mathbf{Z}_p{}^d$ and $H(\mathbf{Q}_p)$ comes from a differential volume form. Consequently their image measure in $\mathbf{Z}_p{}^d$, (resp. $\to \mathbf{Z}_p{}^{\dim(H)}$) will be associated to differential volume forms, hence will have locally bounded above and below density with respect to the Haar measures. Thus we can consider the case of a linear map with respect to the Haar measures $\mathbf{Z}_p{}^d \to \mathbf{Z}_p{}^{\dim(H)}$, in which case the proposition can be check directly. □

Applying Radon-Nykodym theorem, we deduce the following.

Corollary 3.4. — *Let Φ be a rational open map $\mathbf{Z}_p{}^d \to H(\mathbf{Q}_s)$. Then the direct image of the Haar measure of $\mathbf{Z}_p{}^d$ has an essentially nonzero integrable density with respect to the Haar measure of $H(\mathbf{Q}_S)$, and it dominates a measure with essentially nonzero bounded density.*

4. Spaces of lattices, Mahler's criterion

In order to use [**KT07**], we fix here some notations. We refer to [**KT07**], section 8 for the details. Recall that S is assume to contain the archimedean place. Consequently, $\mathbf{Z}_S$ defines a discrete cocompact ring in $\mathbf{Q}_S$. A *lattice* in $\mathbf{Q}_S^m$ will be discrete $\mathbf{Z}_S$-submodule Λ of rank m. Equivalently Λ is a $\mathbf{Z}_S$-module generated by a basis of $\mathbf{Q}_S{}^m$ over $\mathbf{Q}_S$.

We identify the space of lattices in $\mathbf{Q}_S{}^m$ with $GL(m,\mathbf{Z}_S)\backslash GL(m,\mathbf{Q}_S)$ *via* the map

$$GL(m,\mathbf{Z}_S)g \mapsto \mathbf{Z}_S{}^m g.$$

Let λ_v denote the standard Lebesgue measure on $\mathbf{R}$ if v is archimedean, or the additive Haar measure on $\mathbf{Q}_p$ such that $\lambda_v(\mathbf{Z}_p) = 1$ if v is finite and associated with the prime p. We denote by λ_S the product Haar measure on $\mathbf{Q}_S$. Then $\mathbf{Z}_S$ has covolume 1 in $\mathbf{Q}_S$ with respect to λ_S. We endow $\mathbf{Q}_S{}^m$ with the product Haar measure. Then lattices have finite covolume, and for any lattice written as $\mathbf{Z}_S{}^m g$, this covolume is $\left|\det(g)\right|_S$.

As $G(\mathbf{Z}_S)$ is a lattice in $G(\mathbf{Q}_S)$, we know, from Borel and Harish-Chandra criterion that $\det(G) = \{1\}$. Consequently G is contained in $SL(m)$, and the map $GL(\mathbf{Z}_S)g \mapsto {\mathbf{Z}_S}^m g$ identify $G(\mathbf{Z}_S)\backslash G(\mathbf{Q}_S)$ with a space of lattices in ${\mathbf{Q}_S}^m$ of covolume one.

When L is a discrete $\mathbf{Z}_S$-submodule of $\mathbf{Q}_S$, write the subspace $\mathbf{Q}_S L$ generated by L as a sum $\mathbf{Q}_S L = \oplus_{v\in S}(\mathbf{Q}_S L)\otimes\mathbf{Q}_v$, identify each $(\mathbf{Q}_S L)\otimes\mathbf{Q}_v$ with the corresponding subspace of ${\mathbf{Q}_v}^m$, and endow $\mathbf{Q}_S L$ with the Haar measure which is the product measure of, for each factor $(\mathbf{Q}_S L)\otimes\mathbf{Q}_v$, the Haar measure induced

- by the induced euclidean structure from $\mathbf{R}^m$ on $(\mathbf{Q}_S L)\otimes\mathbf{R}$ if v is archimedean;
- the Haar measure on $(\mathbf{Q}_S L)\otimes\mathbf{Q}_v$ giving volume one to $((\mathbf{Q}_S L)\otimes\mathbf{Q}_v)\cap\mathbf{Z}_p^m$ if v is finite and associated with a prime p.

We then define the covolume $\mathrm{cov}(L)$ of L as the covolume of L inside $\mathbf{Q}_S L$ with respect to the above Haar measure.

As a particular case, if L has rank one and generator x, then $\mathrm{cov}(L) = \|x\|_S$ where we define $\|(x_v)_{v\in S}\|_S = \prod_{v\in S}\|x_v\|_v$ where $\|-\|_v$ denote

- the standard euclidean norm if v is archimedean;
- the homogeneous norm unit sphere ${\mathbf{Z}_p}^m \smallsetminus p{\mathbf{Z}_p}^m$ if v is finite and associated with a prime p.

We define the systole function $\mathrm{sys} : G(\mathbf{Z}_S)\backslash G(\mathbf{Q}_S) \to \mathbf{R}$ as $g \mapsto \inf\left\{\|x\|_S \,|\, x \in {\mathbf{Z}_S}^m g \smallsetminus \{0\}\right\}$. Note that this infimum is actually a minimum, because any lattice in ${\mathbf{Q}_S}^m$, being discrete intersect any closed ball in ${\mathbf{Q}_S}^m$, which is compact, along a finite set.

We recall that Mahler's compactness criterion asserts that a subset E in $G(\mathbf{Z}_S)\backslash G(\mathbf{Q}_S)$ is bounded if and only if the systole function is bounded away from zero on this subset. Consequently, a family of measures $(\mu_i)_{i\in I}$ on $G(\mathbf{Z}_S)\backslash G(\mathbf{Q}_S)$ is narrow if and only if

$$\forall \epsilon > 0, \exists \epsilon', \forall i \in I, \mu_i(\{x \in G(\mathbf{Z}_S)\backslash G(\mathbf{Q}_S) \mid \mathrm{sys}(x) \leq \epsilon'\}) < \epsilon. \tag{12}$$

5. A "good" parametrisation

Recall that [**KT07**], section 3, define, on a subset U metric space (X, d) with nowhere zero Borel measure μ, a real nonzero Borel function to be (C,α)-*good* on U, for some positive invertible constants C and α, if for any open ball B in U one has

$$\forall \epsilon > 0, \mu\left(\left\{x \in B \,\middle|\, |f(x)| < \epsilon \cdot \sup_{b\in B}|f(b)|\right\}\right) \leq C\epsilon^\alpha \mu(B). \tag{13}$$

In other words "we can effectively contol, in any ball, the relative time a good function is relatively small".

Consider the class of functions $E(n,\Lambda)$ from [**EMS97**], Definition 1, namely the class of functions $\mathbf{R} \to \mathbf{C}$ made of a linear combination of $t \mapsto t^l \exp(\lambda t)$, with a natural integer l such that $l \leq n$ and a complex parameter λ such that $|\lambda| \leq \Lambda$. Let us prove that for any bounded subset U of $\mathbf{R}$, there exists is some positive invertible

constants C and α such that for any (nonzero) function f in $E(n,\Lambda)$, $\left|f\right|$ is (C,α)-good on U (with respect to the Lebesgue measure).

Proof. — It will be enough to check property (13) for any open ball of bounded radius in $\mathbf{R}$, that is an open interval of bounded length.

Desired result is the content of Corollary 2.10 from [**EMS97**], provided one can effectively bound involved constant M by a polynomial in the ϵ of the statement. From the use of Corollary 2.9 in the proof of Corollary 2.10, the subset

$$\left\{ x \in B \,\middle|\, \left|f(x)\right| < 1/M \cdot \sup_{b\in B} \left|f(b)\right| \right\}$$

is a union of at most n^2-1 subintervals. Assume that $M>1$ so that any of these intervals can be B itself. So each of these subintervals J has a boundary point in B, and consequently $\sup_{b\in J}\left|f(b)\right| = \epsilon \sup_{b\in B}\left|f(b)\right|$. Applying Corollary 2.10 on each of these subintervals, we conclude that M convene for ϵ and $M>1$, then M^2 convene for ϵ^2.

This yields the desire bound and finishes the proof. □

Using Lemma 3.2 from [**KT07**], we deduce that for the any class $E(m,n,\Lambda)$ of multivariate functions $\mathbf{R}^m \to \mathbf{C}$, and for any bounded subset U in $\mathbf{R}^m$, there exists some positive invertible constants C and α such that for any (nonzero) function f in $E(m,n,\Lambda)$, $\left|f\right|$ is (C,α)-good on U for the Lebesgue measure. (Note that any bounded subset of $\mathbf{R}^m$ is contained in a product of bounded subsets of $\mathbf{R}$)

In situation of Lemma 3.1, given Φ, and U as in the Lemma, the Lemmas 3.2 and 3.4 of [**KT07**] implies there exists constants C and α such that for any nonzero function ϕ in Φ, $\left|\phi\right|$ is (C,α)-good on U.

Proposition 5.1. — *Let $\rho : G \to Sl(n)$ be a representation, for some natural integer n. Let $\|-\|_S$ be some norm on $\mathbf{Q}_S{}^n$. Consider, for every place v in S, let Θ_v denote*

- *a generically submersive function (cf.*[**RS09**]*, A.3) of some class $E_G(m,n,\Lambda)$ if v is archimedean;*
- *a function $\mathbf{Z}_p{}^{d_v}$ as in Proposition 3.2 if v is a finite associated with some prime p.*

Let Θ denote the product map $\Theta_S((\lambda_v)_{v\in S} \mapsto \prod_{v\in S}\Theta_v(\lambda_v)$.

Then for any bounded subset U in the domain of Θ, there exists positive and invertible constants C and α such that for any x in $\mathbf{Q}_S{}^n$, and any g in $G(\mathbf{Q}_S)$ the function $\left\|\rho(\Theta g)\cdot x\right\|_S$ is (C,α)-good on U.

Note that the submersivity assumption may always be satisfied. It follows, for exemple from [**RS09**], A.3 and A.4.

Proof. — We first note that, possibly translating x, we may ignore the element g.

Using lemma 3.1 (d) in [**KT07**], we may replace $\|-\|$ by any comparable norm. Consequently, we may assume that $\|-\|_S$ may be written $\prod_{v\in S}\|-\|_v$, with $\|-\|_v$ be the maximum of $|-|_v$ applied to the coordinates.

Using Lemma 3.3 of [**KT07**], we may assume that S contains only one element, say v.

Using Lemma 3.1 (c) in [**KT07**], we may replace the function $\|\Theta\cdot x\|_S$ by the absolute value of some coordinate. Note that coordinates of $\|\Theta\cdot x\|_S$ are matrix coefficients of Θ.

Recall that the class $E_G(m,n,\Lambda)$ is made of functions into G whose matrix coefficients in the adjoint representation of G belongs to $E(m,n,\Lambda)$. As G is semisimple, its adjoint representation is a closed immersion. It follows that any algebraic regular function on G, and in particular the matrix coefficients of ρ, belong to some class $E(m',n',\Lambda)'$. Then for archimedean v, the proposition follows from the preceding discussion.

If v is a finite place, then from Proposition 3.2 and definition (13) we may assume Θ is a polynomial map. It then follows from the use of Lemmas 3.1, 3.3 and 3.4 of [**KT07**] as in the proof of Theorem 9.4 of [**KT07**]. □

6. Proof

Let $n=2^m$ and consider the exterior algebra representation $\rho : GL(m)\to GL(n)$ (written in some basis). As G is contained in $SL(m)$, its image under ρ, and *a fortiori* the image of H is contained in $SL(n)$. Indeed, $\det\circ\rho$ defines a character, hence is trivial on $SL(m)$, the latter being simple.

As in proof of Theorem 9.4 in [**KT07**], there is suitable norm on ${\mathbf{Q}_S}^n$ such that for any discrete $\mathbf{Z}_S$-submodule Δ of ${\mathbf{Q}_S}^n$, there is some x in ${\mathbf{Q}_S}^n$, such that for any g in $GL(m,\mathbf{Q}_S)$,

$$\mathrm{cov}(\Delta g)=\left\|x\rho(g)\right\|_S.$$

We consider a map Θ as in Proposition 5.1. Then there are some positive and invertible constants C and α such that for any discrete $\mathbf{Z}_S$-submodule Δ of ${\mathbf{Q}_S}^n$, and any g in $G(\mathbf{Q}_S)$, the function $\mathrm{cov}(\Delta\Theta g)$ is (C,α)-good. In particular condition (i) of Theorem 9.3 of [**KT07**] is satisfied for the map Θg. Let Y_S be as in Theorem 2.1, and let c be constant as in Theorem 2.1 relative to ρ and the image of the Θ_v (at a finite place v, Θ_v, being open, has Zariski dense image). Then for any y in Y_S, the translated map $\Theta\cdot y$ satisfies the condition (i) and (ii) of Theorem 9.3. Of course we may assume $c<1$.

The other conditions of Theorem 9.3 are satisfied for the same reason as in the proof of Theorem 9.4. We conclude that there is some (effectively computable, cf.[**KT07**] 9.3) constant C' such that for any y in Y_S for any ball B in $\prod_{v\in S}{\mathbf{Q}_v}^{d_v}$ of some radius R at a centre x such that the ball of radius 3^mR at the same centre is

contained in the domain of Θ, we have

$$\forall \epsilon < c\mu(\{b \in B | \mathrm{sys}({\mathbf{Z}_S}^m \Theta(b)\, y) < \epsilon c) \leq C' \epsilon^{\alpha},$$

where μ is a Haar measure on the domain of Θ. By virtue of formula (12), this implies that if μ_B denote the direct image of μ in $G(\mathbf{Z}_S)\backslash G(\mathbf{Q}_S)$, then the family of translates $(\mu_B \cdot y)_{y \in Y_S}$ is narrow.

According Corollary 3.4 and [**RS09**] A.4, the measures μ_B is absolutely continuous, Hence dominate a measure with positive bounded non essentially zero density. Using property (3) concludes the proof of Corollary 1.4.

References

[BGO08] M. BOROVOI, A. GORODNIK & H. OH – "Rational points on homogeneous varieties and Equidistribution of Adelic periods. (with an appendix by m. borovoi)", *prepublication* (As of April 1, 2008).

[BHC62] A. BOREL & HARISH-CHANDRA – "Arithmetic subgroups of algebraic groups", *Ann. of Math. (2)* **75** (1962), p. 485–535.

[EMS97] A. ESKIN, S. MOZES & N. SHAH – "Non-divergence of translates of certain algebraic measures", *Geom. Funct. Anal.* **7** (1997), no. 1, p. 48–80.

[KT07] D. KLEINBOCK & G. TOMANOV – "Flows on S-arithmetic homogeneous spaces and applications to metric Diophantine approximation", *Comment. Math. Helv.* **82** (2007), no. 3, p. 519–581.

[Ric09] R. RICHARD – "Résultat géométrique sur les représentations de groupes algébriques réductifs sur un corps ultramétrique", *Cette thèse* (2009).

[RS09] R. RICHARD & N. SHAH – "Résultat géométrique sur les représentations de groupes de Lie réductifs", *Cette thèse* (2009).

RODOLPHE RICHARD, IRMAR, Bâtiment 22-23, université de Rennes 1, Campus de Beaulieu, 35000 Rennes. • *E-mail :* Rodolphe.RICHARD@Normalesup.org

VU :

Le Directeur de Thèse
(Nom et Prénom)

VU :

Le Responsable de l'École Doctorale

VU pour autorisation de soutenance

Rennes, le

Le Président de l'Université de Rennes 1

Guy CATHELINEAU

VU après soutenance pour autorisation de publication :

Le Président de Jury,
(Nom et Prénom)

Sur quelques questions d'équidistribution en géométrie arithmétique

Résumé – Nous démontrons un résultat d'équidistribution sur les courbes modulaires : les orbites galoisiennes d'invariants modulaires a l'intérieur d'une même classe d'isogénie non CM se répartissent le long de la mesure de Poincaré sur la courbe modulaire. Un corollaire est que la hauteur des points considérés diverge, retrouvant là un résultat de Szpiro et Ullmo. Pour obtenir cet énoncé nous combinons des propriétés galoisiennes (le théoreme de Serre sur l'action du groupe de Galois sur les points de division) et des propriétés ergodiques (le théorème de Ratner sur les flots unipotents dans les espaces de réseaux, ou plutôt l'équidistribution des points de Hecke). Nous généralisons notre méthode dans le cadre des variétés de Shimura. Dans ce cadre, en revanche, l'un de nos ingrédients repose sur une forme de la conjecture de Mumford-Tate.

Cela nous amène à étudier, dans une seconde partie, des raffinements de l'équidistribution des points de Hecke. Apparaissent alors certaines questions de divergence dans les espaces de réseaux. La méthode de linéarisation de Dani-Margulis ramène cette question à un énoncé géométrique. Nous apportons une réponse à cette question. Dans le cas réel, il s'agit d'une collaboration avec Nimish Shah. Dans le cas p-adique, nous sommes amenés à utiliser la géométrie ultramétrique récemment développée par Berkovich, en relation avec la théorie de Bruhat-Tits, et plus particulièrement des résultats recents de B. Remy, A. Thuillier et A. Werner. Nous sommes amenés en particulier à démontrer

- des propriétés de décomposition des immeubles inspirées des théorème de décomposition de Mostow sur les espaces symétriques ;
- des propriétés de convexité sur les immeubles de fonctions analytiques, au sens ultramétrique, sur le groupe associé.

Nous illustrons enfin comment nos résultats, en combinaison avec les travaux de D. Kleinbock et G. Tomanov, et le théorème de Ratner, s'appliquent à l'étude de problèmes S-arithmétiques dans les espaces de réseaux.

On Some Equidistribution Questions in Arithmetic Geometry

Abstract – We prove some equidistribution result on the modular curves: Galois orbits of modular invariants within a same non CM isogeny class distribute along the Poincaré measure on the modular curve. As a corollary, the height of the considered points diverges, recovering a result of Szpiro and Ullmo. To prove such a statement, we combine galois properties (Serre's theorem on the Galois action on division points) and ergodic properties (Ratner's theorem on unipotent flows, or rather the equidistribution of Hecke points). We generalise our method in the setup of Shimura varieties. But in the latter setup, on of our ingredients rely on some variant of Mumford-Tate conjecture.

This brings us to study, in a second part, some refinements of the equidistribution of Hecke points. Some issues of non-divergences in lattices spaces has then to be dealt with. Dani-Margulis linearization tecnhique reduces this to some geometric statement. We provide an answer to this question. In the real case, it is a collaboration with Nimish Shah. In the p-adic case, we are lead to use the ultrametric geometry recently developped by Berkovich, together with Bruhat-Tits theory, and more particularly the recent work of B. Remy, A. Thuillier et A. Werner. We precisely prove

- some decomposition properties in buildings inspired by Mostow decomposition theorem for symmetric spaces;
- some convexity properties, on buildings, for analytic functions, in the ultramétric sense, on the associated group.

We finally illustrate how our results, in combination with D. Kleinbock and G. Tomanov work, and Ratner's theorem, applies to the study of some S-arithmetic problems in lattices spaces.